H.R. 3844, THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT OF 2002

HEARING

BEFORE THE

SUBCOMMITTEE ON GOVERNMENT EFFICIENCY, FINANCIAL MANAGEMENT AND INTERGOVERNMENTAL RELATIONS

OF THE

COMMITTEE ON GOVERNMENT REFORM HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTH CONGRESS

SECOND SESSION

ON

H.R. 3844

TO STRENGTHEN FEDERAL GOVERNMENT INFORMATION SECURITY, INCLUDING THROUGH THE REQUIREMENT FOR THE DEVELOPMENT OF MANDATORY INFORMATION SECURITY RISK MANAGEMENT STANDARDS

MAY 2, 2002

Serial No. 107–190

Printed for the use of the Committee on Government Reform

Available via the World Wide Web: http://www.gpo.gov/congress/house
http://www.house.gov/reform

U.S. GOVERNMENT PRINTING OFFICE

86–343 PDF WASHINGTON : 2003

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON GOVERNMENT REFORM

DAN BURTON, Indiana, *Chairman*

BENJAMIN A. GILMAN, New York
CONSTANCE A. MORELLA, Maryland
CHRISTOPHER SHAYS, Connecticut
ILEANA ROS-LEHTINEN, Florida
JOHN M. MCHUGH, New York
STEPHEN HORN, California
JOHN L. MICA, Florida
THOMAS M. DAVIS, Virginia
MARK E. SOUDER, Indiana
STEVEN C. LATOURETTE, Ohio
BOB BARR, Georgia
DAN MILLER, Florida
DOUG OSE, California
RON LEWIS, Kentucky
JO ANN DAVIS, Virginia
TODD RUSSELL PLATTS, Pennsylvania
DAVE WELDON, Florida
CHRIS CANNON, Utah
ADAM H. PUTNAM, Florida
C.L. "BUTCH" OTTER, Idaho
EDWARD L. SCHROCK, Virginia
JOHN J. DUNCAN, JR., Tennessee

HENRY A. WAXMAN, California
TOM LANTOS, California
MAJOR R. OWENS, New York
EDOLPHUS TOWNS, New York
PAUL E. KANJORSKI, Pennsylvania
PATSY T. MINK, Hawaii
CAROLYN B. MALONEY, New York
ELEANOR HOLMES NORTON, Washington, DC
ELIJAH E. CUMMINGS, Maryland
DENNIS J. KUCINICH, Ohio
ROD R. BLAGOJEVICH, Illinois
DANNY K. DAVIS, Illinois
JOHN F. TIERNEY, Massachusetts
JIM TURNER, Texas
THOMAS H. ALLEN, Maine
JANICE D. SCHAKOWSKY, Illinois
WM. LACY CLAY, Missouri
DIANE E. WATSON, California
STEPHEN F. LYNCH, Massachusetts

BERNARD SANDERS, Vermont
(Independent)

KEVIN BINGER, *Staff Director*
DANIEL R. MOLL, *Deputy Staff Director*
JAMES C. WILSON, *Chief Counsel*
ROBERT A. BRIGGS, *Chief Clerk*
PHIL SCHILIRO, *Minority Staff Director*

SUBCOMMITTEE ON GOVERNMENT EFFICIENCY, FINANCIAL MANAGEMENT AND INTERGOVERNMENTAL RELATIONS

STEPHEN HORN, California, *Chairman*

RON LEWIS, Kentucky
DAN MILLER, Florida
DOUG OSE, California
ADAM H. PUTNAM, Florida

JANICE D. SCHAKOWSKY, Illinois
MAJOR R. OWENS, New York
PAUL E. KANJORSKI, Pennsylvania
CAROLYN B. MALONEY, New York

EX OFFICIO

DAN BURTON, Indiana
HENRY A. WAXMAN, California

J. RUSSELL GEORGE, *Staff Director and Chief Counsel*
EARL PIERCE, *Professional Staff Member*
JUSTIN PAULHAMUS, *Clerk*
MARK STEPHENSON, *Minority Professional Staff Member*

CONTENTS

H.R. 3844, THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT OF 2002

THURSDAY, MAY 2, 2002

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON GOVERNMENT EFFICIENCY, FINANCIAL MANAGEMENT AND INTERGOVERNMENTAL RELATIONS,
COMMITTEE ON GOVERNMENT REFORM,
Washington, DC.

The subcommittee met, pursuant to notice, at 10:02 a.m., in room 2154, Rayburn House Office Building, Hon. Stephen Horn (chairman of the subcommittee) presiding.

Present: Representatives Horn, Davis, Schakowsky, and Turner.

Staff present: J. Russell George, staff director and chief counsel; Bonnie Heald, deputy staff director and communications director; Earl Pierce, professional staff member; Henry Wray, senior counsel; Justin Paulhamus and Teddy Kidd, clerks; Chip Nottingham, counsel; David McMillen and Mark Stephenson, minority professional staff members; and Jean Gosa, minority assistant clerk.

Mr. HORN. A quorum being present, the Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations will come to order.

I am very pleased that we are holding this joint hearing with Chairman Davis and his Subcommittee on Technology and Procurement Policy on H.R. 3844, the Federal Information Security Management Act of 2002.

It is clear from recent hearings held by our subcommittee that agency valuations that the work started in 2000 must be continued. Agencies have not yet developed security plans that balance protection and cost. Few agencies have implemented security controls that are adequate to protect against violations of privacy, data loss, corruption or cyber attacks. The current reporting requirements imposed by the Government Information Security Reform Act have brought the scope and magnitude of security weaknesses into sharp focus in both Congress and the executive branch. This focus is the first crucial step in eliminating security weaknesses.

H.R. 3844 incorporates the key provisions of the Government Information Security Reform Act, including the requirements for risk-based security management, independent evaluations, and reporting of agency security programs. The bill also clarifies some of the language in the original act; it eliminates the sunset provision of the act and adds new provisions to reflect lessons learned during the implementation of the 2000 act.

The purpose of today's hearing is to consider the merits of the legislation and any potential improvements to it. I welcome today's

witnesses and I look forward to working with each of you to ensure the security of the Government's information technology resources.

We are delighted to have the gentleman from Texas, Mr. Turner. He comes from Mr. Davis' committee. We lost him out of our committee and we miss you. Mr. Turner.

[The text of H.R. 3844 follows:]

107TH CONGRESS
2D SESSION

H. R. 3844

To strengthen Federal Government information security, including through the requirement for the development of mandatory information security risk management standards.

IN THE HOUSE OF REPRESENTATIVES

MARCH 5, 2002

Mr. TOM DAVIS of Virginia (for himself and Mr. HORN) introduced the following bill; which was referred to the Committee on Government Reform, and in addition to the Committee on Science, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

---

A BILL

To strengthen Federal Government information security, including through the requirement for the development of mandatory information security risk management standards.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. INFORMATION SECURITY.

(a) SHORT TITLE.—The amendments made by this section may be cited as the "Federal Information Security Management Act of 2002".

(b) INFORMATION SECURITY.—

(1) IN GENERAL.—Subchapter II of chapter 35 of title 44, United States Code, is amended to read as follows:

"SUBCHAPTER II—INFORMATION SECURITY

"§ 3531. Purposes

"The purposes of this subchapter are to—

"(1) provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets;

"(2) recognize the highly networked nature of the current Federal computing environment and provide effective governmentwide management and oversight of the related information security risks, including coordination of information security efforts throughout the civilian, national security, and law enforcement communities;

"(3) provide for development and maintenance of minimum controls required to protect Federal information and information systems; and

"(4) provide a mechanism for improved oversight of Federal agency information security programs.

"§ 3532. Definitions

"(a) IN GENERAL.—Except as provided under subsection (b), the definitions under section 3502 shall apply to this subchapter.

"(b) ADDITIONAL DEFINITIONS.—As used in this subchapter—

"(1) the term 'information security' means protecting information and information systems from unauthorized use, disclosure, disruption, modification, or destruction in order to provide—

"(A) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;

"(B) confidentiality, which means preserving an appropriate level of information secrecy; and

"(C) availability, which means ensuring timely and reliable access to and use of information;

"(2) the term 'national security system' means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—

"(A) the function, operation, or use of which—

"(i) involves intelligence activities;

"(ii) involves cryptologic activities related to national security;

"(iii) involves command and control of military forces;

"(iv) involves equipment that is an integral part of a weapon or weapons system; or

"(v) is critical to the direct fulfillment of military or intelligence missions provided that this definition does not apply to a system that is used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications); or

"(B) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy; and

"(3) the term 'information technology' has the meaning given that term in section 5002 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1401).

"§ 3533. Authority and functions of the Director

"(a) The Director shall oversee agency information security policies and practices, including—

"(1) developing and overseeing the implementation of policies, principles, standards, and guidelines on information security, including through the promulgation of standards and guidelines under section 5131 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1441);

"(2) requiring agencies, consistent with the standards and guidelines promulgated under such section 5131 and the requirements of this subchapter, to identify and provide information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized use, disclosure, disruption, modification, or destruction of—

"(A) information collected or maintained by or on behalf of an agency; or

"(B) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;

"(3) coordinating the development of standards and guidelines under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) with agencies and offices operating or exercising control of national security systems (including the National Security Agency) to assure, to the maximum extent feasible, that such standards and guidelines are complementary with standards and guidelines developed for national security systems;

"(4) overseeing agency compliance with the requirements of this subchapter, including through any authorized action under section 5113(b)(5) of the Clinger-Cohen Act of 1996 (40 U.S.C. 1413(b)(5)) to enforce accountability for compliance with such requirements;

"(5) coordinating information security policies and procedures with related information resources management policies and procedures;

"(6) overseeing the development and operation of the Federal information security incident center established under section 3536; and

"(7) reporting to Congress on agency compliance with the requirements of this subchapter, including—

"(A) a summary of the findings of evaluations required by section 3535;

"(B) significant deficiencies in agency information security practices; and

"(C) planned remedial action to address such deficiencies.

"(b) Except for the authorities described in paragraphs (4) and (7) of subsection (a), the authorities of the Director under this section shall not apply to national security systems.

"§ 3534. Federal agency responsibilities

"(a) The head of each agency shall—

"(1) be responsible for—

"(A) providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized use, disclosure, disruption, modification, or destruction of—

"(i) information collected or maintained by or on behalf of the agency; and

"(ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;

"(B) complying with the requirements of this subchapter and related policies, procedures, standards, and guidelines, including—

"(i) information security standards and guidelines promulgated by the Director under section 5131 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1441); and

"(ii) information security standards and guidelines for national security systems issued in accordance with law and as directed by the President; and

"(C) ensuring that information security management processes are integrated with agency strategic and operational planning processes;

"(2) ensure that senior agency officials provide information security for the information and information systems that support the operations and assets under their control, including through—

"(A) assessing the risk and magnitude of the harm that could result from the unauthorized use, disclosure, disruption, modification, or destruction of such information or information systems;

"(B) determining the levels of information security appropriate to protect such information and information systems in accordance with standards and guidelines promulgated under section 5131 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1441) for information security classifications and related requirements;

"(C) implementing policies and procedures to cost-effectively reduce risks to an acceptable level; and

"(D) periodically testing and evaluating information security controls and techniques to ensure that they are effectively implemented;

"(3) delegate to the agency Chief Information Officer established under section 3506 (or comparable official in an agency not covered by such section) the authority to ensure compliance with the requirements imposed on the agency under this subchapter, including—

"(A) designating a senior agency information security officer who shall—

"(i) carry out the Chief Information Officer's responsibilities under this section;

"(ii) possess professional qualifications, including training and experience,

required to administer the functions described under this section;

"(iii) have information security duties as that official's primary duty; and

"(iv) head an office with the mission and resources to assist in ensuring agency compliance with this section;

"(B) developing and maintaining an agencywide information security program as required by subsection (b);

"(C) developing and maintaining information security policies, procedures, and control techniques to address all applicable requirements, including those issued under section 3533 of this title, and section 5131 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1441);

"(D) training and overseeing personnel with significant responsibilities for information security with respect to such responsibilities; and

"(E) assisting senior agency officials concerning their responsibilities under subparagraph (2);

"(4) ensure that the agency has trained personnel sufficient to assist the agency in complying

with the requirements of this subchapter and related policies, procedures, standards, and guidelines; and

"(5) ensure that the agency Chief Information Officer, in coordination with other senior agency officials, reports annually to the agency head on the effectiveness of the agency information security program, including progress of remedial actions.

"(b) Each agency shall develop, document, and implement an agencywide information security program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source, that includes—

"(1) periodic assessments of the risk and magnitude of the harm that could result from the unauthorized use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency;

"(2) policies and procedures that—

"(A) are based on the risk assessments required by subparagraph (1);

"(B) cost-effectively reduce information security risks to an acceptable level;

"(C) ensure that information security is addressed throughout the life cycle of each agency information system; and

"(D) ensure compliance with—

"(i) the requirements of this subchapter;

"(ii) policies and procedures as may be prescribed by the Director, including information security standards and guidelines promulgated under section 5131 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1441); and

"(iii) any other applicable requirements, including standards and guidelines for national security systems issued in accordance with law and as directed by the President;

"(3) subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate;

"(4) security awareness training to inform personnel, including contractors and other users of information systems that support the operations and assets of the agency, of—

"(A) information security risks associated with their activities; and

"(B) their responsibilities in complying with agency policies and procedures designed to reduce these risks;

"(5) periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed with a frequency depending on risk, but no less than annually;

"(6) a process for ensuring remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency;

"(7) procedures for detecting, reporting, and responding to security incidents, consistent with guidance issued under section 3536, including—

"(A) mitigating risks associated with such incidents before substantial damage is done;

"(B) notifying and consulting with the Federal information security incident center established under section 3536; and

"(C) notifying and consulting with, as appropriate—

"(i) law enforcement agencies and relevant Offices of Inspector General;

"(ii) an office designated by the President for any incident involving a national security system; and

"(iii) any other agency or office, in accordance with law or as directed by the President; and

"(8) plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

"(c) Each agency shall—

"(1) report annually to the Director and the Comptroller General on the adequacy and effectiveness of information security policies, procedures, and practices, including compliance with the requirements of this subchapter;

"(2) address the adequacy and effectiveness of information security policies, procedures, and practices in plans and reports relating to—

"(A) annual agency budgets;

"(B) information resources management under subchapter 1 of this chapter;

"(C) information technology management under the Clinger-Cohen Act of 1996 (40 U.S.C. 1401 et seq.);

"(D) program performance under sections 1105 and 1115 through 1119 of title 31, and sections 2801 and 2805 of title 39;

"(E) financial management under chapter 9 of title 31, and the Chief Financial Officers Act of 1990 (31 U.S.C. 501 note; Public Law 101–576) (and the amendments made by that Act);

"(F) financial management systems under the Federal Financial Management Improvement Act (31 U.S.C. 3512 note); and

"(G) internal accounting and administrative controls under section 3512 of title 31, United States Code, (known as the 'Federal Managers Financial Integrity Act'); and

"(3) report any significant deficiency in a policy, procedure, or practice identified under paragraph (1) or (2)—

"(A) as a material weakness in reporting under section 3512 of title 31, United States Code; and

"(B) if relating to financial management systems, as an instance of a lack of substantial compliance under the Federal Financial Man-

agement Improvement Act (31 U.S.C. 3512 note).

"(d)(1) In addition to the requirements of subsection (c), each agency, in consultation with the Director, shall include as part of the performance plan required under section 1115 of title 31 a description of—

"(A) the time periods, and

"(B) the resources, including budget, staffing, and training,

that are necessary to implement the program required under subsection (b).

"(2) The description under paragraph (1) shall be based on the risk assessments required under subsection (b)(2)(1).

"(e) Each agency shall provide the public with timely notice and opportunities for comment on proposed information security policies and procedures to the extent that such policies and procedures affect communication with the public.

"§ 3535. Annual independent evaluation

"(a)(1) Each year each agency shall have performed an independent evaluation of the information security program and practices of that agency to determine the effectiveness of such program and practices.

"(2) Each evaluation by an agency under this section shall include—

"(A) testing of the effectiveness of information security policies, procedures, and practices of a representative subset of the agency's information systems;

"(B) an assessment (made on the basis of the results of the testing) of compliance with—

"(i) the requirements of this subchapter; and

"(ii) related information security policies, procedures, standards, and guidelines; and

"(C) separate presentations, as appropriate, regarding information security relating to national security systems.

"(b) Subject to subsection (c)—

"(1) for each agency with an Inspector General appointed under the Inspector General Act of 1978, the annual evaluation required by this section shall be performed by the Inspector General or by an independent external auditor, as determined by the Inspector General of the agency; and

"(2) for each agency to which paragraph (1) does not apply, the head of the agency shall engage

an independent external auditor to perform the evaluation.

"(c) For each agency operating or exercising control of a national security system, that portion of the evaluation required by this section directly relating to a national security system shall be performed—

"(1) only by an entity designated by the agency head; and

"(2) in such a manner as to ensure appropriate protection for information associated with any information security vulnerability in such system commensurate with the risk and in accordance with all applicable laws.

"(d) The evaluation required by this section—

"(1) shall be performed in accordance with generally accepted government auditing standards; and

"(2) may be based in whole or in part on an audit, evaluation, or report relating to programs or practices of the applicable agency.

"(e) The results of an evaluation required by this section shall be submitted to the Director no later than March 1, 2003, and every March 1 thereafter.

"(f) Agencies and evaluators shall take appropriate steps to ensure the protection of information which, if disclosed, may adversely affect information security. Such

protections shall be commensurate with the risk and comply with all applicable laws and regulations.

"(g)(1) The Director shall summarize the results of the evaluations conducted under this section in a report to Congress.

"(2) The Director's report to Congress under this subsection shall summarize information regarding information security relating to national security systems in such a manner as to ensure appropriate protection for information associated with any information security vulnerability in such system commensurate with the risk and in accordance with all applicable laws.

"(3) Evaluations and any other descriptions of information systems under the authority and control of the Director of Central Intelligence or of National Foreign Intelligence Programs systems under the authority and control of the Secretary of Defense shall be made available to Congress only through the appropriate oversight committees of Congress, in accordance with applicable laws.

"(h) The Comptroller General shall periodically evaluate and report to Congress on—

"(1) the adequacy and effectiveness of agency information security policies and practices; and

"(2) implementation of the requirements of this subchapter.

"§ 3536. Federal information security incident center

"(a) The Director shall cause to be established and operated a central Federal information security incident center to—

"(1) provide timely technical assistance to operators of agency information systems regarding security incidents, including guidance on detecting and handling information security incidents;

"(2) compile and analyze information about incidents that threaten information security;

"(3) inform operators of agency information systems about current and potential information security threats, and vulnerabilities; and

"(4) consult with agencies or offices operating or exercising control of national security systems (including the National Security Agency) and such other agencies or offices in accordance with law and as directed by the President regarding information security incidents and related matters.

"(b) Each agency operating or exercising control of a national security system shall share information about information security incidents, threats, and vulnerabilities with the Federal information security incident center to the extent consistent with standards and guidelines for national security systems, issued in accordance with law and as directed by the President.

"§ 3537. National security systems

"The head of each agency operating or exercising control of a national security system shall be responsible for ensuring that the agency—

"(1) provides information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized use, disclosure, disruption, modification, or destruction of the information contained in such system;

"(2) implements information security policies and practices as required by standards and guidelines for national security systems, issued in accordance with law and as directed by the President; and

"(3) complies with the requirements of this subchapter.

"§ 3538. Authorization of appropriations

"There are authorized to be appropriated to carry out the provisions of this subchapter such sums as may be necessary for each of fiscal years 2003 through 2007.".

(2) CLERICAL AMENDMENT.—The items in the table of sections at the beginning of such chapter 35 under the heading "SUBCHAPTER II" are amended to read as follows:

"3531. Purposes.
"3532. Definitions.
"3533. Authority and functions of the Director.
"3534. Federal agency responsibilities.
"3535. Annual independent evaluation.

(c) INFORMATION SECURITY RESPONSIBILITIES OF CERTAIN AGENCIES.—

(1) NATIONAL SECURITY RESPONSIBILITIES.—(A) Nothing in this Act (including any amendment made by this Act) shall supersede any authority of the Secretary of Defense, the Director of Central Intelligence, or other agency head, as authorized by law and as directed by the President, with regard to the operation, control, or management of national security systems, as defined by section 3532(3) of title 44, United States Code.

(B) Section 2224 of title 10, United States Code, is amended—

(i) in subsection 2224(b), by striking "(b) OBJECTIVES AND MINIMUM REQUIREMENTS.—(1)" and inserting "(b) OBJECTIVES OF THE PROGRAM.—";

(ii) in subsection 2224(b), by striking "(2) the program shall at a minimum meet the requirements of section 3534 and 3535 of title 44, United States Code."; and

(iii) in subsection 2224(c), by inserting ", including through compliance with subtitle II

of chapter 35 of title 44" after "infrastructure".

(2) ATOMIC ENERGY ACT OF 1954.—Nothing in this Act shall supersede any requirement made by or under the Atomic Energy Act of 1954 (42 U.S.C. 2011 et seq.). Restricted Data or Formerly Restricted Data shall be handled, protected, classified, downgraded, and declassified in conformity with the Atomic Energy Act of 1954 (42 U.S.C. 2011 et seq.).

SEC. 2. MANAGEMENT OF INFORMATION TECHNOLOGY.

Section 5131 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1441) is amended to read as follows:

"SEC. 5131. RESPONSIBILITIES FOR FEDERAL INFORMATION SYSTEMS STANDARDS.

"(a)(1)(A) Except as provided under paragraph (3), the Director of the Office of Management and Budget shall, on the basis of standards and guidelines developed by the National Institute of Standards and Technology pursuant to paragraphs (2) and (3) of section 20(a) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3(a)) and in consultation with the Secretary of Commerce, promulgate standards and guidelines pertaining to Federal information systems.

"(B) Standards promulgated under subparagraph (A) shall include—

"(i) standards that provide minimum information security requirements as determined under section 20(b) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3(b)); and

"(ii) such standards that are otherwise necessary to improve the efficiency of operation or security of Federal information systems.

"(C) Standards described under subparagraph (B) shall be compulsory and binding.

"(D) The President may disapprove or modify such standards and guidelines if the President determines such action to be in the public interest. The President's authority to disapprove or modify such standards and guidelines may not be delegated. Notice of such disapproval or modification shall be published promptly in the Federal Register. Upon receiving notice of such disapproval or modification, the Director shall immediately rescind or modify such standards or guidelines as directed by the President.

"(2) Standards and guidelines for national security systems, as defined under section 3532(3) of title 44, United States Code, shall be developed, promulgated, enforced, and overseen as otherwise authorized by law and as directed by the President.

"(b) The head of an agency may employ standards for the cost-effective information security for all operations and assets within or under the supervision of that agency that are more stringent than the standards promulgated by the Director under this section, if such standards—

"(1) contain, at a minimum, the provisions of those applicable standards made compulsory and binding by the Director; and

"(2) are otherwise consistent with policies and guidelines issued under section 3533 of title 44, United States Code.

"(c) The promulgation of any standard or guideline by the Director under subsection (a), and the disapproval of any standard or guideline by the President under subsection (a)(1)(C), shall occur no later than 6 months after the submission of such standard or guideline to the Director by the National Institute of Standards and Technology, as provided under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3).".

SEC. 3. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY.

Section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3), is amended by striking the text and inserting the following:

"(a) The Institute shall—

"(1) have the mission of developing standards, guidelines, and associated methods and techniques for information systems;

"(2) develop standards and guidelines, including minimum requirements, for information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency, other than national security systems (as defined in section 3532(b)(2) of title 44, United States Code); and

"(3) develop standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets, but such standards and guidelines shall not apply to national security systems.

"(b) The standards and guidelines required by subsection (a) shall include, at a minimum—

"(1)(A) standards to be used by all agencies to categorize all information and information systems collected or maintained by or on behalf of each agen-

cy based on the objectives of providing appropriate levels of information integrity, confidentiality, and availability according to a range of risk levels;

"(B) guidelines recommending the types of information and information systems to be included in each such category; and

"(C) minimum information security requirements for information and information systems in each such category;

"(2) a definition of and guidelines concerning detection and handling of information security incidents; and

"(3) guidelines for identifying an information system as a national security system.

"(c) In developing standards and guidelines required by subsection (a), the Institute shall—

"(1) consult with other agencies and offices (including, but not limited to, the Director of the Office of Management and Budget, the Departments of Defense and Energy, the National Security Agency, and the General Accounting Office) to assure—

"(A) use of appropriate information security policies, procedures, and techniques, in order to improve information security and avoid

unnecessary and costly duplication of effort; and

"(B) that such standards and guidelines are complementary with standards and guidelines employed for the protection of national security systems and information contained in such systems;

"(2) submit to the Director of the Office of Management and Budget for promulgation under section 5131 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1441)—

"(A) standards, as required under subsection (b)(1)(A), no later than 12 months after the date of the enactment of this section;

"(B) guidelines, as required under subsection (b)(1)(B), no later than 18 months after the date of the enactment of this Act; and

"(C) minimum information security requirements for each category, as required under subsection (b)(1)(C), no later than 36 months after the date of the enactment of this section; and

"(3) emphasize the development of policies and procedures that do not require specific technical solutions or products.

"(d)(1) There is established in the Institute an Office for Information Security Programs.

"(2) The Office for Information Security Programs shall be headed by a Director, who shall be a senior executive and shall be compensated at a level in the Senior Executive Service under section 5382 of title 5, United States Code, as determined by the Secretary of Commerce.

"(3) The Director of the Institute shall delegate to the Director of the Office of Information Security Programs the authority to administer all functions under this section, except that any such delegation shall not relieve the Director of the Institute of responsibility for the administration of such functions. The Director of the Office of Information Security Programs shall serve as principal adviser to the Director of the Institute on all functions under this section.

"(e) The Institute shall—

"(1) submit standards and guidelines developed pursuant to subsection (a), along with recommendations as to the extent to which these should be made compulsory and binding, to the Director of the Office of Management and Budget for promulgation under section 5131 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1441);

"(2) provide assistance to agencies regarding—

"(A) compliance with the standards and guidelines developed under subsection (a);

"(B) detecting and handling information security incidents; and

"(C) information security policies, procedures, and practices;

"(3) conduct research, as needed, to determine the nature and extent of information security vulnerabilities and techniques for providing cost-effective information security;

"(4) develop and periodically revise performance indicators and measures for agency information security policies and practices;

"(5) evaluate private sector information security policies and practices and commercially available information technologies to assess potential application by agencies to strengthen information security;

"(6) solicit and consider the recommendations of the Information Security Advisory Board, established by section 21, regarding standards and guidelines that are being considered for submittal to the Director of the Office of Management and Budget in accordance with paragraph (1) and submit such recommendations to the Director of the Office of Man-

agement and Budget with such standards and guidelines submitted to the Director; and

"(7) report annually to the Director of the Office of Management and Budget on—

"(A) compliance with the requirements of this section, the Clinger-Cohen Act of 1996 (40 U.S.C. 1401 et seq.), and other related requirements;

"(B) major deficiencies in Federal information security; and

"(C) recommendations to improve Federal information security.

"(f) As used in this section—

"(1) the term 'agency' has the same meaning as provided in section 3502(1) of title 44, United States Code;

"(2) the term 'information security' has the same meaning as provided in section 3532(1) of such title;

"(3) the term 'information system' has the same meaning as provided in section 3502(8) of such title;

"(4) the term 'information technology' has the same meaning as provided in section 5002 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1401); and

"(5) the term 'national security system' has the same meaning as provided in section 3532(b)(2) of such title.

"(g) There are authorized to be appropriated to the Secretary of Commerce $20,000,000 for each of fiscal years 2003, 2004, 2005, 2006, and 2007 to enable the National Institute of Standards and Technology to carry out the provisions of this section.".

SEC. 4. INFORMATION SECURITY ADVISORY BOARD.

Section 21 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–4), is amended—

(1) in subsection (a), by striking "Computer System Security and Privacy Advisory Board" and inserting "Information Security Advisory Board";

(2) in subsection (a)(1), by striking "computer or telecommunications" and inserting "information technology";

(3) in subsection (a)(2)—

(A) by striking "computer or telecommunications technology" and inserting "information technology"; and

(B) by striking "computer or telecommunications equipment" and inserting "information technology";

(4) in subsection (a)(3)—

(A) by striking "computer systems" and inserting "information system"; and

(B) by striking "computer systems security and privacy" and inserting "information security";

(5) in subsection (b)(1) by striking "computer systems security and privacy" and inserting "information security";

(6) in subsection (b) by striking paragraph (2) and inserting the following:

"(2) to advise the Institute and the Director of the Office of Management and Budget on information security issues pertaining to Federal Government information systems, including through review of proposed standards and guidelines developed by the Director of the National Institute of Standards and Technology under section 20; and";

(7) in subsection (b)(3) by inserting "annually" after "report";

(8) by inserting after subsection (e) the following new subsection:

"(f) The Board shall hold meetings at such locations and at such time and place as determined by a majority of the Board.";

(9) by redesignating subsections (f) and (g) as subsections (g) and (h), respectively;

(10) by striking subsection (h), as redesignated by paragraph (9), and inserting the following:

"(h) As used in this section, the terms "information system" and "information technology" have the meanings given in section 20."; and

(11) by inserting at the end the following:

"(i) There are authorized to be appropriated to the Secretary of Commerce $1,250,000 for each of fiscal years 2003, 2004, 2005, 2006, and 2007 to enable the Information Security Advisory Board to identify emerging issues related to information security, and to convene public meetings on those subjects, receive presentations, and publish reports and recommendations for public distribution.".

SEC. 5. TECHNICAL AND CONFORMING AMENDMENTS.

(a) COMPUTER SECURITY ACT.—Sections 5 and 6 of the Computer Security Act of 1987 (40 U.S.C. 1441 note) are repealed.

(b) FLOYD D. SPENCE NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2001.—The Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001 (Public Law 106–398) is amended by striking subtitle G of title X.

(c) PAPERWORK REDUCTION ACT.—(1) Section 3504(g) of title 44, United States Code, is amended—

(A) by adding "and" at the end of paragraph (1);

(B) in paragraph (2)—

(i) by striking "sections 5 and 6 of the Computer Security Act of 1987 (40 U.S.C. 759 note)" and inserting "subchapter II of this title"; and

(ii) by striking the semicolon and inserting a period; and

(C) by striking paragraph (3).

(2) Section 3506(g) of such title is amended—

(A) by adding "and" at the end of paragraph (1);

(B) in paragraph (2)—

(i) by striking "the Computer Security Act of 1987 (40 U.S.C. 759 note)" and inserting "subchapter II of this title"; and

(ii) by striking the semicolon and inserting a period; and

(C) by striking paragraph (3).

SEC. 6. EFFECTIVE DATE.

This Act and the amendments made by this Act shall take effect 30 days after the date of the enactment of this Act.

○

Mr. TURNER. Thank you, Mr. Chairman. It is good to be at a hearing with you again because it was a pleasure to serve with you on your committee during the last Congress.

I understand your committee has had a number of hearings on the issue of computer security. You have done some very hard work on the issue and I commend you for the attention you have paid to this very important matter. I thank you for scheduling a joint hearing with our committee.

This legislation, the Federal Information Security Management Act was introduced by the chairman of our subcommittee, Tom Davis. I want to thank Mr. Davis for his efforts and his work with the minority in working on the various provisions of the bill. This legislation, as we know, will permanently authorize the information security program evaluation and reporting requirements of the Government Information Security Reform Act that became law about 18 months ago and will expire at the end of November.

This law has proved to be very useful in focusing agencies' attention to the critical issue of computer security by requiring annual reports to the Office of Management and Budget. The bill would make a number of changes designed to strengthen information security across the Federal Government including the development of minimum information security standards by the National Institute of Standards and Technology, creation of a Federal Information Security Incident Center, and clarification of the definition of national security systems. Most importantly, it would require that the reports under this bill would go not only to OMB but to the Comptroller General of the General Accounting Office to facilitate better congressional oversight of computer security.

Again, Chairman Horn, I commend you on your leadership on this issue and I commend Chairman Davis for his sponsorship of the legislation.

I yield back. Thank you, Mr. Chairman.

[The prepared statement of Hon. Jim Turner follows:]

Statement of Rep. Jim Turner
Joint Hearing on H.R. 3844, the Federal Information
Security Management Act

May 2, 2002

Thank you Chairman Horn. It's good to be in a hearing with you again. I understand that you have held a number of hearings on the issue of computer security and have issued one of your famous report cards grading agencies on the matter. You have done much hard work on the issue and I commend you for your attention to this important matter.

Today's hearing is on H.R. 3844, the Federal Information Security Management Act, introduced by Chairman Davis. I want to thank Mr. Davis for his efforts to consult with the minority as this bill was being drafted. The intention was to develop a bill that we could all support, and I think he has in large part succeeded.

H.R. 3844 would permanently authorize the information security program, evaluation, and reporting requirements of the Government Information Security Reform Act, which became law about 18months ago and is due to expire at the end of November this year. That law has proved useful in focusing agency's attention on the critical issue of computer security by requiring annual reports to the Office of Management and Budget. H.R. 3844 would also make a number of changes designed to

strengthen information security across the federal government, including the development of minimum information security standards by the National Institute of Standards and Technology, creation of a federal information security incident center, and clarification of the definition of national security systems. The bill also, and I think importantly, requires agencies to report to both OMB and to the Comptroller General at GAO, which would facilitate better Congressional oversight of computer security.

Thank you Mr. Chairman. I look forward to hearing from our witnesses today.

Mr. HORN. Thank you.

I am delighted now to greet our Co-Chairman, the gentleman from Virginia.

Mr. DAVIS. Good morning.

I want to thank you for holding this hearing in a joint format and for your many years of leadership on the issues of information security and improved government management.

I would also like to thank the distinguished group of witnesses who have joined us today to share their expertise on the issue of government information security, as well as for your specific comments on H.R. 3844.

Government information security is not a new issue to this committee and it is certainly not a new issue to our witnesses today. Billions of dollars have been spent over the years, numerous legislative administrative initiatives have been implemented and some of the best thinking and most respected expertise on information security has been cultivated by our Federal Government in an ongoing effort to protect our information technology systems from intrusion and tampering.

Overall, I believe that our Federal workers and managers deserve enormous credit for adopting to the complex and fast-moving changes that have been thrust upon our government by the information technology revolution. Similarly, I believe we are on the right track in strengthening our management information security. Clearly this administration, represented by several talented leaders here today, is taking this issue seriously and is working harder than ever to better secure our Federal Government's information assets.

While today's discussion focuses on just one bill that will extend and hopefully improve the existing information security management process, it was first codified 2 years ago with the enactment of GISRA. We should not lose sight of the big picture, the fact that our Nation is facing a growing and very real threat from those who seek to harm us by targeting our information systems in an effort to disrupt and disable the effective operation of our government. Every day we learn of new attacks on our information systems and every day IT experts, managers and procurement officers are working to stay one step ahead of the threat.

That is why it is critically important for Congress to lend a hand in providing direction that brings coordination, increased management attention and real accountability to the Federal information security sector. I believe it would be a mistake for Congress to micromanage the executive branch's efforts in this area and we need to avoid the temptation to prescribe a rigid, one-size fits all standard that is likely to become outdated quickly as technology and know-how evolve.

At the same time, I am not satisfied with our Federal Government's overall performance in securing our information infrastructure. The bottom line is, we are still too vulnerable. Record IT security expenditures and unprecedented attention to IT security, while important indicators of level of effort, are not the benchmarks we should use to determine success. Instead, we need to focus on developing strong, risk-based, agency-wide security management programs that cover all operations and assets of our Federal agencies.

In addition, new legislative guidance is needed to require the development, promulgation and compliance with mandatory management controls for securing information systems and managing risks as determined by agencies.

I think H.R. 3844 clarifies and strengthens the existing Government Information Security Reform Act of 2000 in four major ways. Under FISMA, we included a number of provisions that require the development, promulgation and compliance with minimum mandatory management controls for securing information. For example, NIST would be required to develop mandatory information security standards for all agencies. Second, agencies would be required to submit an annual report featuring the results of agency evaluations of information security to both OMB and the Comptroller General. Third, the treatment of national security systems would be clarified by removing the term "mission critical system" and replacing it with "national security system." This means that only truly national security and intelligence related information systems would be exempt from information security risk management requirements. Fourth, OMB would oversee the establishment of a central Federal Information Security Incident Center that would inform agencies about information security, threats and vulnerabilities and provide technical assistance to agencies.

In future years, all of us involved with setting and implementing security policy during these challenging times will be faced with the question did we do enough to safeguard our critical information structure. I believe that FISMA will go a long way toward allowing us to honestly answer that question in the affirmative.

I look forward to our hearing today, to improving this legislation if needed, and to ultimately bringing it forward to enactment.

Thank you.

[The prepared of Hon. Tom Davis follows:]

May 2, 2002

STATEMENT OF CONGRESSMAN TOM DAVIS ON H.R. 3844, THE "FEDERAL INFORMATION SECURITY MANAGEMENT ACT OF 2002" AT THE JOINT HEARING OF THE SUBCOMMITTEE ON GOVERNMENT EFFICIENCY, FINANCIAL MANAGEMENT, AND INTERGOVERNMENTAL RELATIONS AND THE SUBCOMMITTEE ON TECHNOLOGY AND PROCUREMENT POLICY

Good morning. Let me begin by thanking Chairman Horn for holding this hearing in a joint format and for his many years of leadership on the issues of information security and improved government management. I would also like to thank the distinguished group of witnesses who have joined us today to share their expertise on the issue of government information security as well as their specific comments on H.R. 3844.

Government information security is not a new issue to this committee and it is certainly not a new issue to our witnesses today. Billions of dollars have been spent over the years, numerous legislative and administrative initiatives have been implemented, and some of the best thinking and most respected expertise on information security has been cultivated by our federal government in an ongoing effort to protect our information technology systems from intrusion and tampering. Overall, I believe that our federal workers and managers deserve enormous credit for adapting to the complex and fast-moving changes that have been thrust upon our government by the information technology revolution. Similarly, I believe that we are on the right track in strengthening our management of information security. Clearly, this Administration, represented by several talented leaders here today, is taking this issue seriously and is working harder than ever to better secure our federal government information assets.

While today's discussion focuses on just one bill that would extend, and hopefully improve, the existing information security management process that was first codified two years ago with enactment of the Government Information Security Reform Act of 2000 (a.k.a. "GISRA"), we should not lose sight of the big picture – the fact that our nation is facing a growing and very real threat from those that seek to harm us by targeting our information systems in an effort to disrupt and disable the effective operation of our government. Every day we learn of new attacks on our information systems and every day government I.T. experts, managers, and procurement officers are working to stay one step ahead of the threat.

That is why it is critically important for Congress to lend a hand in providing direction that brings coordination, increased management attention, and real accountability to the federal information security sector. I believe that it would be a mistake for Congress to micromanage the Executive Branch's efforts in this area, and we need to avoid the temptation to prescribe a rigid "once size fits all" approach that is likely to become outdated quickly as technology and know-how evolve. At the same time, however, I am not satisfied with our federal government's overall performance in securing our information infrastructure. The bottom line is that we are still too vulnerable. Record I.T. security expenditures and unprecedented attention to I.T. security (while important indicators of "level of effort") are not the benchmarks that we should use to determine success. Instead, we need to focus on developing strong, risk-based, agency-wide security management programs that cover all operations and assets of federal agencies. In addition, new legislative guidance is needed to require the development, promulgation, and compliance with minimum mandatory management controls for securing information systems and managing risks as determined by agencies.

H.R. 3844 clarifies and strengthens the existing Government Information Security Reform Act of 2000 in four major ways: Under H.R. 3844 (FISMA):

1) Includes a number of provisions that require the development, promulgation, and compliance with minimum mandatory management controls for securing information. For example, NIST would be required to develop mandatory minimum information security requirements for all agencies.
2) Agencies would be required to submit an annual report featuring the results of agency evaluations of information security to both OMB and the comptroller general.
3) The treatment of national security systems would be clarified by removing the term "mission critical system" and replacing it with "national security system." This means that only truly national security and intelligence related information systems would be exempt from information security risk management requirements.
4) OMB would oversee the establishment of a central federal information security incident center that would inform agencies about information security threats and vulnerabilities and provide technical assistance to agencies.

In future years, all of us involved with setting and implementing information security policy during these challenging times will be faced with the question: "Did we do enough to safeguard our critical information infrastructure?" I believe that the Federal Information Security Management Act of 2002 will go a long way towards allowing us to honestly answer this question in the affirmative. I look forward to our hearing today and to improving this legislation, if needed, and to ultimately bringing it forward for enactment.

Thank you.

Mr. HORN. We will begin with panel one. Our first witness, and not a stranger to these committees, is Robert F. Dacey, Director, Information Security, U.S. General Accounting Office, headed by the Comptroller General of the United States. We appreciate all the work the GAO does. We will announce one of their books as we end this particular hearing.

STATEMENTS OF ROBERT F. DACEY, DIRECTOR, INFORMATION SECURITY, U.S. GENERAL ACCOUNTING OFFICE; MARK A. FORMAN, ASSOCIATE DIRECTOR, INFORMATION TECHNOLOGY AND E-GOVERNMENT, OFFICE OF MANAGEMENT AND BUDGET; DANIEL G. WOLF, DIRECTOR, INFORMATION ASSURANCE DIRECTORATE, NATIONAL SECURITY AGENCY; BENJAMIN H. WU, DEPUTY UNDER SECRETARY, COMMERCE FOR TECHNOLOGY ADMINISTRATION, DEPARTMENT OF COMMERCE; RONALD E. MILLER, CHIEF INFORMATION OFFICER, FEDERAL EMERGENCY MANAGEMENT AGENCY; DAVID C. WILLIAMS, TREASURY INSPECTOR GENERAL, TAX ADMINISTRATION; AND JAMES X. DEMPSEY, DEPUTY DIRECTOR, CENTER FOR DEMOCRACY AND TECHNOLOGY

Mr. DACEY. I am pleased to be here today to discuss the proposed Federal Information Security Management Act of 2002, FISMA. As you requested, I will briefly summarize my written statement.

Since September 1996, we have reported that poor information security is a widespread Federal problem with potentially devastating consequences. Although agencies have taken steps to redesign and strengthen their information security programs, our analyses of information security at major agencies have shown that Federal systems were not being adequately protected from computer-based threats, even though these systems process, store and transmit enormous amounts of sensitive data and are indispensable to many Federal operations.

Concerned with these reports, Congress passed into law the Government Information Security Reform provisions commonly referred to as GISRA to reduce these risks and provide more effective oversight of Federal information security. First year implementation of GISRA represented a significant step in improving Federal agency information security programs and addressing longstanding weaknesses.

For example, agencies have noted benefits from GISRA such as increased management attention to and accountability for information security and have stated that as a result of implementing GISRA, they are taking significant steps to improve their information security programs. Agency IGs also view GISRA as a positive step toward improving information security, also noting the increased management attention.

In addition, the administration has taken important actions to address information security such as plans to integrate information security into the President's management agenda scorecard. Such benefits and planned actions demonstrate the importance of GISRA's requirements and the significant impact they have had on information security in the Federal Government.

FISMA would permanently authorize and strengthen the information security program, evaluation and reporting requirements

established by GISRA which is to expire in November of this year. We believe the continued authorization of such important information security legislation is essential to sustaining agency efforts to identify and correct significant weaknesses.

Further, this authorization would reinforce the Federal Government's commitment to establishing information security as an integral part of its operations and help ensure that the administration and Congress continue to receive the information they need to effectively manage and oversee Federal information security.

FISMA continues several important GISRA provisions, including requiring agency program managers and CIOs to implement a risk-based security management program covering all operations of the agency; second, requiring an independent annual evaluation of each agency's information security program; third, taking a governmentwide approach to information security by accommodating a wide range of information security needs and applying requirements to all agencies, including those involved in national security; and fourth, through annual reporting requirements, providing a means for both OMB and the Congress to oversee the effectiveness of agency and governmentwide information security, measure progress in improving information security, and consider information security in budget deliberations.

FISMA also proposes a number of changes and clarifications to strengthen information security, some of which address issues noted in the first year implementation of GISRA. In particular, the bill requires the development, promulgation and compliance with minimum mandatory management controls for securing information and information systems, creates the requirement for annual agency reporting to both OMB and the Comptroller General, and clarifies the definition of and evaluation of responsibilities for national security systems. In addition, the bill proposes other changes that would require Federal agencies to strengthen their information security programs, update the information and security responsibilities missed, and clarify other otherwise streamline definitions and legislative language.

In addition to reauthorizing information security legislation, there are a number of other important steps the administration and agencies should take to ensure information security receives appropriate attention and resources and that known deficiencies are addressed. These include delineating the roles and responsibilities of the numerous entities involved in Federal information security and related aspects of critical infrastructure protection; obtaining adequate technical expertise to select, implement, and maintain controls to protect information systems and allocating sufficient agency resources for information security.

As the chairman noted, later today the committee will be releasing a report which summarizes our testimony on March 6 and makes certain recommendations for improving GISRA and its implementation.

Mr. Chairman, this concludes my statement. I would be pleased to answer any questions that you or the Members may have.

[The prepared statement of Mr. Dacey follows:]

United States General Accounting Office

GAO

Testimony

Before the Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations and the Subcommittee on Technology and Procurement Policy, Committee on Government Reform, House of Representatives

For Release on Delivery
Expected at
10 a.m. EDT
Thursday,
May 2, 2002

INFORMATION SECURITY

Comments on the Proposed Federal Information Security Management Act of 2002

Statement of Robert F. Dacey
Director, Information Security Issues

GAO-02-677T

Messrs. Chairmen and Members of the Subcommittees:

I am pleased to be here today to discuss H.R. 3844, the Federal Information Security Management Act of 2002. This bill seeks to strengthen federal government information security by reauthorizing and expanding the information security, evaluation, and reporting requirements enacted into law as the Government Information Security Reform provisions (commonly referred to as "GISRA") in the National Defense Authorization Act for Fiscal Year 2001.[1] Concerned with reports that continuing, pervasive information security weaknesses place federal operations at significant risk of disruption, tampering, fraud, and inappropriate disclosures of sensitive information, the Congress enacted GISRA to reduce these risks and provide more effective oversight of federal information security.

As I stated in my March 6, 2002, testimony before the Government Efficiency, Financial Management and Intergovernmental Relations Subcommittee, first-year implementation of GISRA represented a significant step in improving federal agencies' information security programs and addressing their serious, pervasive information security weaknesses.[2] However, first-year implementation indicated areas in which GISRA could be strengthened and clarified to further improve federal information security and congressional oversight. Furthermore, GISRA will expire on November 29, 2002, less than a year away.

In my testimony today, I will first discuss the need to continue authorization of government information security legislation in view of the major information security risks that are facing federal agencies. Next, I will discuss major changes proposed in H.R. 3844, such as requiring annual agency reporting to the Office of Management and Budget (OMB) and the comptroller general, and establishing mandatory minimum security controls. Finally, I will highlight other changes in H.R. 3844 intended to clarify and streamline GISRA provisions.

Messrs. Chairmen, this testimony is based on our analysis of the proposed language of H.R. 3844 that you introduced in the House of Representatives on March 5, 2002. It is also based on the results of our review of first-year

[1]Title X, Subtitle G—Government Information Security Reform, Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001, P.L. 106-398, October 30, 2000.

[2]U.S. General Accounting Office, *Information Security: Additional Actions Needed to Fully Implement Reform Legislation*, GAO-02-470T (Washington, D.C.: Mar. 6, 2002).

GISRA implementation as presented in my March 2002 testimony and in our report, which is being released today entitled, *Information Security: Additional Actions Needed to Fully Implement Reform Legislation*.[3] We performed our work during March and April 2002 in accordance with generally accepted government auditing standards.

Results In Brief

H.R. 3844 would permanently authorize and strengthen the information security program, evaluation, and reporting requirements established by GISRA, which is to expire on November 29, 2002. As demonstrated by first-year implementation, GISRA proved to be a significant step in improving federal agencies' information security programs and addressing their serious, pervasive information security weaknesses. Agencies have noted benefits from GISRA, such as increased management attention to and accountability for information security. In addition, the administration has taken important actions to address information security, such as plans to integrate information security into the President's Management Agenda Scorecard. We believe that continued authorization of such important information security legislation is essential to sustaining agency efforts to identify and correct significant weaknesses. Further, this authorization would reinforce the federal government's commitment to establishing information security as an integral part of its operations and help ensure that the administration and the Congress continue to receive the information they need to effectively manage and oversee federal information security.

H.R. 3844 also proposes a number of changes and clarifications to strengthen information security, some of which address issues noted in the first-year implementation. In particular, the bill requires the development, promulgation, and compliance with minimum mandatory management controls for securing information and information systems; creates a requirement for annual agency reporting to both OMB and the comptroller general; and clarifies the definition of and evaluation responsibilities for national security systems. In addition, the bill proposes other changes that would require federal agencies to strengthen their information security programs, update the information security responsibilities of the National Institute of Standards and Technology (NIST), and clarify or otherwise streamline definitions and legislative language.

[3]GAO-02-407, Washington, D.C.: May 2, 2002.

In addition to reauthorizing information security legislation, there are a number of important steps that the administration and the agencies should take to ensure that information security receives appropriate attention and resources and that known deficiencies are addressed. These include delineating the roles and responsibilities of the numerous entities involved in federal information security and related aspects of critical infrastructure protection, using the audit results provided by information security legislation for congressional and administration oversight, and allocating sufficient agency resources for information security.

Background

Dramatic increases in computer interconnectivity, especially in the use of the Internet, continue to revolutionize the way our government, our nation, and much of the world communicate and conduct business. However, this widespread interconnectivity also poses significant risks to our computer systems and, more important, to the critical operations and infrastructures they support, such as telecommunications, power distribution, public health, national defense (including the military's warfighting capability), law enforcement, government, and emergency services. Likewise, the speed and accessibility that create the enormous benefits of the computer age, if not properly controlled, allow individuals and organizations to inexpensively eavesdrop on or interfere with these operations from remote locations for mischievous or malicious purposes, including fraud or sabotage.

As greater amounts of money are transferred through computer systems, as more sensitive economic and commercial information is exchanged electronically, and as the nation's defense and intelligence communities increasingly rely on commercially available information technology, the likelihood increases that information attacks will threaten vital national interests. Further, the events of September 11, 2001, underscored the need to protect America's cyberspace against potentially disastrous cyber attacks—attacks that could also be coordinated to coincide with physical terrorist attacks to maximize the impact of both.

Since September 1996, we have reported that poor information security is a widespread federal problem with potentially devastating consequences.[4] Although agencies have taken steps to redesign and strengthen their information system security programs, our analyses of information security at major federal agencies have shown that federal systems were

[4]U.S. General Accounting Office, *Information Security: Opportunities for Improved OMB Oversight of Agency Practices.* GAO/AIMD-96-110 (Washington, D.C.: Sept. 24, 1996).

not being adequately protected from computer-based threats, even though these systems process, store, and transmit enormous amounts of sensitive data and are indispensable to many federal agency operations. In addition, in both 1998 and 2000, we analyzed audit results for 24 of the largest federal agencies and found that all 24 had significant information security weaknesses.[5] As a result of these analyses, we have identified information security as a governmentwide high-risk issue in reports to the Congress since 1997—most recently in January 2001.[6]

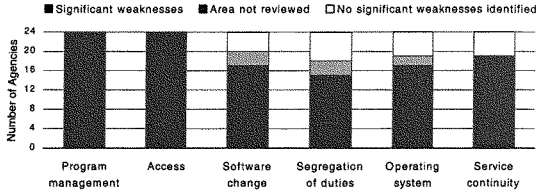
These weaknesses continue as indicated by our most recent analyses for these 24 large federal agencies that considered the results of inspector general (IG) and GAO audit reports published from July 2000 through September 2001, including the results of the IGs' independent evaluations of these agencies' information security programs performed as required by GISRA.[7] These analyses showed significant information security weaknesses in all major areas of the agencies' general controls, that is, the policies, procedures, and technical controls that apply to all or a large segment of an entity's information systems and help ensure their proper operation. Figure 1 illustrates the distribution of weaknesses across the 24 agencies for the following six general control areas: (1) security program management, which provides the framework for ensuring that risks are understood and that effective controls are selected and properly implemented; (2) access controls, which ensure that only authorized individuals can read, alter, or delete data; (3) software development and change controls, which ensure that only authorized software programs are implemented; (4) segregation of duties, which reduces the risk that one individual can independently perform inappropriate actions without detection; (5) operating systems controls, which protect sensitive programs that support multiple applications from tampering and misuse; and (6) service continuity, which ensures that computer-dependent operations experience no significant disruptions.

[5]U.S. General Accounting Office, *Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk*, GAO/AIMD-98-92 (Washington, D.C.: Sept. 23, 1998); *Information Security: Serious and Widespread Weaknesses Persist at Federal Agencies*, GAO/AIMD-00-295 (Washington, D.C.: Sept. 6, 2000).

[6]U.S. General Accounting Office, *High-Risk Series: Information Management and Technology*, GAO/HR-97-9 (Washington, D.C.: Feb. 1, 1997); *High-Risk Series: An Update*, GAO/HR-99-1 (Washington, D.C.: Jan. 1999); *High Risk Series: An Update*, GAO-01-263 (Washington, D.C.: Jan. 2001).

[7]U.S. General Accounting Office, *Computer Security: Improvements Needed to Reduce Risk to Critical Federal Operations and Assets*, GAO-02-231T (Washington, D.C.: Nov. 9, 2001).

Figure 1: Information Security Weaknesses at 24 Major Agencies



Source: Audit reports issued July 2000 through September 2001.

Our analyses showed that weaknesses were most often identified for security program management and access controls. For security program management, we found weaknesses for all 24 agencies in 2001 as compared to 21 agencies (88 percent) in a similar analysis in 2000.[8] For access controls, we also found weaknesses for all 24 agencies in 2001—the same condition we found in 2000.

Concerned with accounts of attacks on commercial systems via the Internet and reports of significant weaknesses in federal computer systems that make them vulnerable to attack, on October 30, 2000, the Congress enacted GISRA, which became effective November 29, 2000, and is in effect for 2 years after this date. GISRA supplements information security requirements established in the Computer Security Act of 1987, the Paperwork Reduction Act of 1995, and the Clinger-Cohen Act of 1996 and is consistent with existing information security guidance issued by OMB[9] and NIST,[10] as well as audit and best practice guidance issued by

[8]U.S. General Accounting Office, *Computer Security: Critical Federal Operations and Assets Remain at Risk*, GAO/T-AIMD-00-314 (Washington, D.C.: Sept. 11, 2000).

[9]Primarily OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources," February 1996.

[10]Numerous publications made available at http://www.itl.nist.gov/ including National Institute of Standards and Technology, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, NIST Special Publication 800-14, September 1996.

GAO.[11] Most importantly, however, GISRA consolidates these separate requirements and guidance into an overall framework for managing information security and establish new annual review, independent evaluation, and reporting requirements to help ensure agency implementation and both OMB and congressional oversight.

The legislation assigned specific responsibilities to OMB, agency heads and chief information officers (CIOs), and the IGs. OMB is responsible for establishing and overseeing policies, standards, and guidelines for information security. This includes the authority to approve agency information security programs, but delegates OMB's responsibilities regarding national security systems to national security agencies. OMB is also required to submit an annual report to the Congress summarizing results of agencies' evaluations of their information security programs. GISRA does not specify a date for this report.

Each agency, including national security agencies, is to establish an agencywide risk-based information security program to be overseen by the agency CIO and ensure that information security is practiced throughout the life cycle of each agency system. Specifically, this program is to include

- periodic risk assessments that consider internal and external threats to the integrity, confidentiality, and availability of systems, and to data supporting critical operations and assets;
- the development and implementation of risk-based, cost-effective policies and procedures to provide security protections for information collected or maintained by or for the agency;
- training on security responsibilities for information security personnel and on security awareness for agency personnel;
- periodic management testing and evaluation of the effectiveness of policies, procedures, controls, and techniques;
- a process for identifying and remediating any significant deficiencies;
- procedures for detecting, reporting and responding to security incidents; and
- an annual program review by agency program officials.

[11]U.S. General Accounting Office, *Federal Information System Controls Audit Manual, Volume 1—Financial Statement Audits*, GAO/AIMD-12.19.6 (Washington, D.C.: Jan. 1999); *Information Security Management: Learning from Leading* Organizations, GAO/AIMD-98-68 (Washington, D.C.: May 1998).

In addition to the responsibilities listed above, GISRA requires each agency to have an annual independent evaluation of its information security program and practices, including control testing and compliance assessment. The evaluations of non–national-security systems are to be performed by the agency IG or an independent evaluator, and the results of these evaluations are to be reported to OMB. For the evaluation of national security systems, special provisions include designation of evaluators by national security agencies, restricted reporting of evaluation results, and an audit of the independent evaluation performed by the IG or an independent evaluator. For national security systems, only the results of each audit of an evaluation are to be reported to OMB.

Finally, GISRA also assigns additional responsibilities for information security policies, standards, guidance, training, and other functions to other agencies. These agencies are NIST, the Department of Defense, the intelligence community, the Attorney General (Department of Justice), the General Services Administration, and the Office of Personnel Management.

H.R. 3844 Would Continue Benefits of Information Security Reform

With GISRA expiring on November 29, 2002, H.R. 3844 proposes to permanently authorize information security legislation that essentially retains the same purposes as GISRA, as well as many of GISRA's information security program, evaluation, and reporting requirements. It would also authorize funding to carry out its provisions for 5 years, thereby providing for periodic congressional oversight of the implementation and effectiveness of these requirements.

We believe that continued authorization of information security legislation is essential to improving federal information security. As emphasized in our March 2002 testimony, the initial implementation of GISRA was a significant step for agencies, the administration, and the Congress in addressing the serious, pervasive weaknesses in the federal government's information security.[12] GISRA consolidated security requirements that existed in law and policy before this law and put into law the following important additional requirements, which are continued in H.R. 3844.

First, GISRA requires agency program managers and CIOs to implement a risk-based security management program covering all operations and assets of the agency and those others provide or manage for the agency. Instituting such an approach is important since many agencies had not effectively evaluated their information security risks and implemented

[12]GAO-02-470T, March 6, 2002.

appropriate controls. Our studies of public and private best practices have shown that effective security program management requires implementing a process that provides for a cycle of risk management activities as now included in GISRA.[13] Moreover, other efforts to improve agency information security will not be fully effective and lasting unless they are supported by a strong agencywide security management program.

Second, GISRA requires an annual independent evaluation of each agency's information security program. Individually, as well as collectively, these evaluations can provide much needed information for improved oversight by OMB and the Congress. Our years of auditing agency security programs have shown that independent tests and evaluations are essential to verifying the effectiveness of computer-based controls. Audits can also evaluate an agency's implementation of management initiatives, thus promoting management accountability. Annual independent evaluations of agency information security programs will help drive reform because they will spotlight both the obstacles and progress toward improving information security and provide a means of measuring progress, much like the financial statement audits required by the Government Management Reform Act of 1994. Further, independent reviews proved to be an important mechanism for monitoring progress and uncovering problems that needed attention in the federal government's efforts to meet the Year 2000 computing challenge.[14]

Third, GISRA takes a governmentwide approach to information security by accommodating a wide range of information security needs and applying requirements to all agencies, including those engaged in national security. This is important because the information security needs of civilian agency operations and those of national security operations have converged in recent years. In the past, when sensitive information was more likely to be maintained on paper or in stand-alone computers, the main concern was data confidentiality, especially as it pertained to classified national security data. Now, virtually all agencies rely on interconnected computers to maintain information and carry out operations that are essential to their missions. While the confidentiality needs of these data vary, all agencies must be concerned about the

[13]General Accounting Office, GAO/AIMD-98-68, Washington, D.C.: May 1998; *Information Security Risk Management: Practices of Leading Organizations*, GAO/AIMD-00-33 (Washington, D.C.: November 1999).

[14]U.S. General Accounting Office, *Year 2000 Computing Challenge: Lessons Learned Can Be Applied to Other Management Challenges*, GAO/AIMD-00-290 (Washington, D.C.: Sept. 12, 2000).

integrity and the availability of their systems and data. It is important for all agencies to understand these various types of risks and take appropriate steps to manage them.

Fourth, the annual reporting requirements provide a means for both OMB and the Congress to oversee the effectiveness of agency and governmentwide information security, measure progress in improving information security, and consider information security in budget deliberations. In addition to management reviews, annual IG reporting of the independent evaluation results to OMB and OMB's reporting of these results to the Congress provide an assessment of agencies' information security programs on which to base oversight and budgeting activities. Such oversight is essential for holding agencies accountable for their performance, as was demonstrated by the OMB and congressional efforts to oversee the Year 2000 computer challenge. This reporting also facilitates a process to help ensure consistent identification of information security weaknesses by both the IG and agency management.

The first-year implementation of GISRA also yielded significant benefits in terms of agency focus on information security. A number of agencies stated that as a result of implementing GISRA, they are taking significant steps to improve their information security programs. For example, one agency stated that the legislation provided it with the opportunity to identify some systemic program-level weaknesses for which it plans to undertake separate initiatives targeted specifically to improve the weaknesses. Other benefits agencies observed included (1) higher visibility of information security within the agencies, (2) increased awareness of information security requirements among department personnel, (3) recognition that program managers are to be held accountable for the security of their operations, (4) greater agency consideration of security throughout the system life cycle, and (5) justification for additional resources and funding needed to improve security. Agency IGs also viewed GISRA as a positive step toward improving information security particularly by increasing agency management's focus on this issue.

Implementation of GISRA has also resulted in important actions by the administration which, if properly carried out, should continue to improve information security in the federal government. For example, OMB has issued guidance that information technology investments will not be funded unless security is incorporated into and funded as part of each investment, and NIST has established a Computer Security Expert Assist Team to review agencies' computer security management. The administration also has plans to

- direct large agencies to undertake a review to identify and prioritize critical assets within the agencies and to identify their interrelationships with other agencies and the private sector;
- conduct a cross-government review to ensure that all critical government processes and assets have been identified;
- integrate security into the President's Management Agenda Scorecard;
- develop workable measures of performance;
- develop electronic training on mandatory topics, including security; and
- explore methods to disseminate vulnerability patches to agencies more effectively.

Such benefits and planned actions demonstrate the importance of GISRA's requirements and the significant impact they have had on information security in the federal government.

Major Changes Proposed by H.R. 3844

H.R. 3844 proposes a number of changes and clarifications that we believe could strengthen information security requirements, some of which address issues noted in the first-year implementation of GISRA.

Establishing Mandatory Minimum Controls

Currently, agencies have wide discretion in deciding what computer security controls to implement and the level of rigor with which to enforce these controls. In theory, some discretion is appropriate since, as OMB and NIST guidance state, the level of protection that agencies provide should be commensurate with the risk to agency operations and assets. In essence, one set of specific controls will not be appropriate for all types of systems and data. Nevertheless, our studies of best practices at leading organizations have shown that more specific guidance is important.[15] In particular, specific mandatory standards for specified risk levels can clarify expectations for information protection, including audit criteria; provide a standard framework for assessing information security risk; help ensure that shared data are appropriately and consistently protected; and reduce demands for already limited agency information security resources to independently develop security controls.

In response to this need, H.R. 3844 includes a number of provisions that would require the development, promulgation, and compliance with minimum mandatory management controls for securing information and

[15]GAO/AIMD-98-68, May 1998.

information systems to manage risks as determined by agencies. Specifically,

- NIST, in coordination with OMB, would be required to develop (1) standards and guidelines for categorizing the criticality and sensitivity of agency information according to the control objectives of information integrity, confidentiality, and availability, and a range of risk levels, and (2) minimum information security requirements for each information category.
- OMB would issue standards and guidelines based on the NIST-developed information and would require agencies to comply with them. This increases OMB's information security authority, given that the secretary of commerce is currently required by the Computer Security Act to issue such standards. These standards would include (1) minimum mandatory requirements and (2) standards otherwise considered necessary for information security.
- Agencies may use more stringent standards than provided by NIST, but H.R. 3844 would require building more stringent protections on top of minimum requirements depending on the nature of information security risks.
- Waiver of the standards is not permitted—they are intended to provide a consistent information security approach across all agencies, while meeting the mission-specific needs of each agency. Thus, agencies would be required to categorize their information and information systems according to control objectives and risk levels and to meet the minimum information security requirements.

Reporting Information to the Congress

H.R. 3844 seeks to improve accountability and congressional oversight by clarifying agency reporting requirements and ensuring that the Congress and GAO have access to information security evaluation results. In particular, it requires agencies to submit an annual report to both OMB and the comptroller general. This reporting requirement is in addition to the requirement in both GISRA and H.R. 3844 that IGs report the results of independent evaluations to OMB and would help to ensure that the Congress receives the information it needs for oversight of federal information security and related budget deliberations. However, to ensure that agencies provide consistent and meaningful information in their reports, it would be important that any such reporting requirement consider specifying what these reports should address.

As reported in our March 2002 testimony, during first-year implementation of GISRA, OMB informed the agencies that it considered GISRA material the CIOs prepared for OMB to be predecisional and not releasable the public, the Congress, or GAO.[16] OMB also considered agencies' corrective action plans to contain predecisional budget information and would not authorize agencies to release them to us. Later, OMB did authorize the agencies to provide copies of their executive summaries, and through continued negotiations with OMB since our March testimony, many agencies are now providing us with the more detailed information that they submitted to OMB. We are continuing to work with OMB to obtain appropriate information from agencies' first-year GISRA corrective action plans and to develop a process whereby this information can be routinely provided to the Congress in the future.

The Congress should have consistent and timely information for overseeing agencies' efforts to implement information security requirements and take corrective actions, as well as for budget deliberations. In our report being released today, we recommend that OMB authorize the heads of federal departments and agencies to release information from their corrective action plans to the Congress and GAO that would (1) identify specific weaknesses to be addressed, their relative priority, the actions to be taken, and the timeframes for completing these actions and (2) provide their quarterly updates on the status of completing these actions.[17] One way to help ensure that the Congress receives such information would be to specifically require that agencies to report it to the Congress and GAO.

Responsibilities for National Security Systems

In our March 2002 testimony, we reported that we were unable to obtain complete information on GISRA implementation for national security systems. Specifically, OMB did not summarize the overall results of the audits of the evaluations for national security systems in its report to the Congress,[18] and the director of central intelligence declined to provide information for our review. In this regard, our report being released today includes a recommendation that OMB provide the Congress with appropriate summary information on the results of the audits of the evaluations for information security programs for national security systems.

[16]GAO-02-470T, March 6, 2002.

[17]GAO-02-407, May 2, 2002.

[18]Office of Management and Budget, *FY 2001 Report to the Congress on Federal Government Information Security Reform*, February 2002.

While we were unable to evaluate this aspect of GISRA implementation, H.R. 3844 proposes to modify GISRA in a number of ways to clarify the treatment of national security systems and to simplify statutory requirements while maintaining protection for the unique requirements of such systems within the risk management approach of the law.

First, the bill replaces GISRA's use of the term "mission critical system." Instead, H.R. 3844 uses the traditional term "national security system." H.R. 3844's use of "national security system," maintaining the longstanding statutory treatment of military and intelligence mission-related systems and classified systems.[19] It would also eliminate a separate category of systems included in GISRA's definition of mission critical system—debilitating impact systems—that broadened the exemption from GISRA for these systems.[20]

Second, consistent with the traditional definitions of national security systems, H.R. 3844 provides more straightforward distinctions between national security and non–national-security systems. This simplifies the law and could simplify compliance for agencies operating national security systems. The bill, for example, replaces GISRA's delegation of policy and oversight responsibilities for national security systems from OMB to national security agencies by simply continuing longstanding limitations on OMB and NIST authority over national security systems.

Third, H.R. 3844 makes a number of changes to GISRA to streamline agency evaluation requirements that affect national security systems:

- The bill clarifies procedures for evaluating national security systems within the context of agencywide evaluations.
- The results of the evaluations of national security systems, not the evaluations themselves, are to be submitted to OMB, which will then prepare a summary report for the Congress. As in GISRA, the actual evaluations and any descriptions of intelligence-related national security systems are to be made available to the Congress only through the intelligence committees.

[19]This two-part definition includes (1) the national security system definition for military and intelligence mission-related systems, and (2) the classified system definition for systems that are protected at all times by procedures established for information that has been appropriately authorized to be kept secret in the interest of national defense or foreign policy.

[20]GISRA defines debilitating impact systems as systems that process information, "the loss, misuse, disclosure, or unauthorized access to or modification of would have a debilitating impact on the mission of the agency."

- The requirement for an audit of the evaluation of national security systems is eliminated. Instead, agencies are required to provide appropriate protections for national security information and, as discussed above, submit only the results of the evaluations to OMB.

We agree that these changes provide a more traditional definition of national security systems, and that such systems should be appropriately considered within the context of a comprehensive evaluation of agency information security. We also believe that requirements for reporting evaluation results to OMB and for OMB to prepare a summary report for the Congress would provide information needed for congressional oversight. This reporting requirement and is consistent with our recommendation contained in the report that we are issuing today: that OMB provide the Congress with appropriate summary information on evaluation results for national security systems.

Additional Agency Requirements Strengthen Information Security Programs

A number of provisions in the proposed legislation establish additional requirements for federal agencies that we believe would strengthen implementation and management of their information security programs. Some of the more significant requirements are as follows:

- Agencies would be required to comply with all standards applicable to their systems, including the proposed mandatory minimum control requirements and those for national security systems. Thus, in implementing an agencywide risk-management approach to information security, agencies with both national security and non–national-security systems would need to have an agencywide information security program that can address the security needs and standards for both kinds of systems.
- Under the bill, the requirement for designating a senior agency information security officer is more detailed than that under GISRA. This official is to (1) carry out the CIO's responsibilities under the act; (2) possess appropriate professional qualifications; (3) have information security as his or her primary duty; and (4) head an information security office with the mission and resources needed to help ensure agency compliance with the act.
- H.R. 3844 also requires each agency to document its agencywide security program and prepare subordinate plans as needed for networks, facilities, and systems. GISRA uses both the terms "security program" and "security plan" and does not specifically require that the program be documented. Our guidance for auditing information system controls states that entities

should have a written plan that clearly describes the entity's security program and policies and procedures that support it.[21]

- H.R. 3844 stresses the importance of agencies having plans and procedures to ensure the continuity of operations for information systems that support the operations and assets of the agency. Such plans, procedures, and other service continuity controls are important because they help ensure that when unexpected events occur, critical operations will continue without undue interruption and that crucial, sensitive data are protected. Losing the capability to process, retrieve, and protect electronically maintained information can significantly affect an agency's ability to accomplish its mission. If service continuity controls are inadequate, even relatively minor interruptions can result in lost or incorrectly processed data, which can cause financial losses, expensive recovery efforts, and inaccurate or incomplete information. For some operations, such as those involving health care or safety, system interruptions could even result in injuries or loss of life. GAO and IG audit work indicate that most of the 24 large agencies we reviewed had weaknesses in service continuity controls, such as plans that were incomplete or not fully tested.

Updating the Mission of NIST and Its Advisory Board

H.R. 3844 maintains NIST's standards development mission for information systems, federal information systems, and federal information security (except for national security and classified systems), but updates the mission of NIST. Some of H.R. 3844's more significant changes to NIST's role and responsibilities would require NIST to:

- develop mandatory minimum information security requirements and guidance for detecting and handling of information security incidents and for identifying an information system as a national security system;
- establish a NIST Office for Information Security Programs to be headed by a senior executive level director; and
- report annually to OMB to create a more active role for NIST in governmentwide information security oversight and to help ensure that OMB receives regular updates on the state of federal information security.

In addition, H.R. 3844 would revise the National Institute of Standards and Technology Act to rename NIST's Computer System Security and Privacy

[21]U.S. General Accounting Office, *Federal Information System Controls Audit Manual, Volume 1—Financial Statement Audits*, GAO/AIMD-12.19.6 (Washington, D.C.: January 1999).

Advisory Board as the Information Security Advisory Board and to ensure that this board has sufficient independence and resources to consider information security issues and provide useful advice to NIST. The bill would strengthen the role of the board by (1) mandating that it provide advice not only to NIST in developing standards, but also to OMB who promulgates such standards; (2) requiring that it prepare an annual report; and (3) authorizing it to hold its meetings where and when it chooses.

Other Changes to Clarify and Streamline the Law

Our analysis of H.R. 3844 identified other proposed changes and requirements that could enhance federal information security, as well as help improve compliance by clarifying inconsistent and unclear terms and provisions, streamlining a number of GISRA requirements, and repealing duplicative provisions in the Computer Security Act and the Paperwork Reduction Act. These changes include the following:

Information security: H.R. 3844 would create a definition for the term "information security" to address three widely accepted objectives—integrity, confidentiality, and availability. Including these objectives in statute highlights that information security involves not only protecting information from disclosure (confidentiality), but also protecting the ability to use and rely on information (availability and integrity).

Information technology: H.R. 3844 would retain GISRA's use of the Clinger-Cohen Act definition of "information technology." However, H.R. 3844 clarifies the scope of this term by using consistent references to "information systems used or operated by any agency or by a contractor of an agency or other organization on behalf of an agency." This emphasizes that H.R. 3844 is intended to cover all systems used by or on behalf of agencies, not just those operated by agency personnel. As discussed previously, both OMB's and GAO's analyses of agencies' first-year GISRA reporting showed significant weaknesses in information security management of contractor-provided or -operated systems.

Independent evaluations: The legislation would continue the GISRA requirement for an annual independent evaluation of each agency's information security program and practices. However, several language changes are proposed to clarify this requirement. For example, the word "representative" would be substituted for "appropriate" in the requirement that the evaluation involve the examination of a sample of systems or procedures. In addition, the bill would also require that the evaluations be performed in accordance with generally accepted government auditing standards, and that GAO periodically evaluate agency information security policies and practices. We agree with these proposed changes to

independent evaluations, but as noted in our March 2002 testimony, these evaluations and expanded coverage for all agency systems under GISRA and H.R. 3844 will also place a significant burden on existing audit capabilities and will require ensuring that agency IGs have necessary resources to either perform or contract for the needed work.[22]

Federal information security incident center. The bill would direct OMB to oversee the establishment of a central federal information security incident center and expands GISRA references to this function. While not specifying which federal agency should operate this center, H.R. 3844 specifies that the center would

- provide timely technical assistance to agencies and other operators of federal information systems;
- compile and analyze information security incident information;
- inform agencies about information security threats and vulnerabilities; and
- consult with national security agencies and other appropriate agencies, such as an infrastructure protection office.

H.R. 3844 would also require that agencies with national security systems share information security information with the center to the extent consistent with standards and guidelines for national security systems. This provision should encourage interagency communication and consultation, while preserving the discretion of national security agencies to determine appropriate information sharing.

Technical and conforming amendments. In addition to its substantive provisions, H.R. 3844 would make a number of minor changes to GISRA and other statutes to ensure consistency within and across these laws. These changes include the elimination of certain provisions in the Paperwork Reduction Act and the Computer Security Act that are replaced by the requirements of GISRA and H.R. 3844.

[22]GAO-02-470T, March 6, 2002.

Improvements Underway, But Challenges to Federal Information Security Remain

As discussed previously, GISRA established important program, evaluation, and reporting requirements for information security; and the first-year implementation of GISRA has resulted in a number of important administration actions and significant agency benefits. In addition, H.R. 3844 would continue and strengthen these requirements to further improve federal information security. However, even with these and other information security-related improvement efforts undertaken in the past few years—such as the president's creation of the Office of Homeland Security and the President's Critical Infrastructure Protection Board—challenges remain.

Given the events of September 11, and reports that critical operations and assets continue to be highly vulnerable to computer-based attacks, the government still faces a challenge in ensuring that risks from cyber threats are appropriately addressed in the context of the broader array of risks to the nation's welfare. Accordingly, it is important that federal information security efforts be guided by a comprehensive strategy for improvement. In 1998, shortly after the initial issuance of Presidential Decision Directive (PDD) 63 on protecting the nation's critical infrastructure, we recommended that OMB, which, by law, is responsible for overseeing federal information security, and the assistant to the president for national security affairs work together to ensure that the roles of new and existing federal efforts were coordinated under a comprehensive strategy.[23] Our later reviews of the National Infrastructure Protection Center and of broader federal efforts to counter computer-based attacks showed that there was a continuing need to clarify responsibilities and critical infrastructure protection objectives.[24]

As I emphasized in my March 2002 testimony, as the administration refines the strategy that it has begun to lay out in recent months, it is imperative that it take steps to ensure that information security receives appropriate attention and resources and that known deficiencies are addressed.[25] These steps would include the following:

[23]U.S. General Accounting Office, *Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk.* GAO/AIMD-98-92 (Washington, D.C.: Sept. 23, 1998).

[24]U.S. General Accounting Office, *Critical Infrastructure Protection: Significant Challenges in Developing National Capabilities.* GAO-01-323 (Washington, D.C.: Apr. 25, 2001); *Combating Terrorism: Selected Challenges and Related Recommendations.* GAO-01-822 (Washington, D.C.: Sept. 20, 2001).

[25]GAO-02-470T, March 6, 2002.

- It is important that the federal strategy delineate the roles and responsibilities of the numerous entities involved in federal information security and related aspects of critical infrastructure protection. Under current law, OMB is responsible for overseeing and coordinating federal agency security, and NIST, with assistance from the National Security Agency, is responsible for establishing related standards. In addition, interagency bodies—such as the CIO Council and the entities created under PDD 63 on critical infrastructure protection—are attempting to coordinate agency initiatives. Although these organizations have developed fundamentally sound policies and guidance and have undertaken potentially useful initiatives, effective improvements are not yet taking place. Further, it is unclear how the activities of these many organizations interrelate, who should be held accountable for their success or failure, and whether they will effectively and efficiently support national goals.
- Ensuring effective implementation of agency information security and critical infrastructure protection plans will require active monitoring by the agencies to determine if milestones are being met and testing to determine if policies and controls are operating as intended. Routine periodic audits, such as those required by GISRA, would allow for more meaningful performance measurement. In addition, the annual evaluation, reporting, and monitoring process established through these provisions, is an important mechanism, previously missing, to hold agencies accountable for implementing effective security and to manage the problem from a governmentwide perspective.
- Agencies must have the technical expertise they need to select, implement, and maintain controls that protect their information systems. Similarly, the federal government must maximize the value of its technical staff by sharing expertise and information. Highlighted during the Year 2000 challenge, the availability of adequate technical and audit expertise is a continuing concern to agencies.
- Agencies can allocate resources sufficient to support their information security and infrastructure protection activities. Funding for security is already embedded to some extent in agency budgets for computer system development efforts and routine network and system management and maintenance. However, some additional amounts are likely to be needed to address specific weaknesses and new tasks. OMB and congressional oversight of future spending on information security will be important to ensuring that agencies are not using the funds they receive to continue ad hoc, piecemeal security fixes that are not supported by a strong agency risk management process.
- Expanded research is needed in the area of information systems protection. While a number of research efforts are underway, experts have

noted that more is needed to achieve significant advances. As the director of the CERT® Coordination Center[26] testified before this subcommittee last September, "It is essential to seek fundamental technological solutions and to seek proactive, preventive approaches, not just reactive, curative approaches." In addition, in its December 2001 third annual report, the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction (also known as the Gilmore Commission) recommended that the Office of Homeland Security develop and implement a comprehensive plan for research, development, test, and evaluation to enhance cyber security.[27]

In summary, the first-year implementation of GISRA has resulted in a number of benefits and positive actions, but much work remains to be done to achieve the objectives of this legislation. Continued authorization of federal information security legislation is essential to sustain agencies' efforts to implement good security practices and to identify and correct significant weaknesses. This reauthorization will also help reinforce the federal government's commitment to establishing information security as an integral part of its operations, as well as help ensure that the administration and the Congress receive the information they need to effectively manage and oversee federal information security.

The changes in requirements, responsibilities, and legislative language proposed in H.R. 3844 would further strengthen the implementation and oversight of information security in the federal government, particularly in establishing mandatory minimum controls and creating reporting requirements to ensure that the Congress receives the information it needs for oversight and budget deliberations related to federal information security. In addition, other changes proposed by H.R. 3844 would clarify and streamline the law and could increase agency compliance with information security requirements. At the same time, with the increasing threat to critical federal operations and assets and poor federal information security, it is imperative that the administration and the

[26]CERT® Coordination Center (CERT-CC) is a center of Internet security expertise located at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University.

[27]*Third Annual Report to the President and Congress of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction*, December 15, 2001.

agencies implement a comprehensive strategy for improvement that emphasizes information security and addresses known weaknesses.

Messrs. Chairmen, this concludes my statement. I would be pleased to answer any questions that you or other members of the subcommittees may have at this time.

Contact

If you should have any questions about the testimony, please contact me at (202) 512-3317. I can be reached by e-mail at *daceyr@gao.gov*.

(310158)

Mr. HORN. Thank you very much. As usual, the GAO comes through.

Now we have a new person with a rich background, Mark A. Forman, Associate Director, Information and Technology and E-Government, Office of Management and Budget. He knows more about any of these problems I think than all the rest of us put together. He created and lead the IBM Americas Public Sector E-Business Consultant Services, was senior professional staff member of our Senate portion of the other body, Senate Governmental Affairs Committee. He has been deeply involved in both the Congress and the executive branch. We are glad to have you here.

Mr. FORMAN. Thank you. I am glad to be here and I appreciate you inviting me to discuss the Federal Information Security Management Act and the administration's views.

I also want to thank your committee and Chairman Davis' committee for the continued vigilance on government computer security. I have been in my job now for 10 months and we have had three hearings on this. It is becoming almost quarterly and I actually think that is good that we have that continued oversight.

We at OMB and other administration officials have discussed components of the Federal Information Security Management Act with your staff and we are still developing an administration position on the bill. As you will hear from my agency colleagues today, there are many divergent views on various provisions. We look forward to working with you and Chairman Davis to make the bill successful as it moves through the legislative process.

As you know, the President has given a high priority to the security of government assets as well as improving the overall management performance of Executive agencies. These priorities are interrelated. As I discussed this March before the committee, our review of agency security programs found that most security issues in the government are fundamentally management issues. We are tracking progress on both issues through use of the executive branch score card for the President's management agenda. If an agency does not meet the IT security criteria, it will not achieve a green score, regardless of their performance under the other e-government criteria.

OMB reported in our February 13 Security Benchmark Report to Congress on Government Information Security that as is, the current state of security across the Federal enterprise is poor. We reported on six fundamental governmentwide weaknesses as well as agency-specific gaps. We find those weaknesses are pervasive and many exist across the Federal community, including the national security community. We found that agencies must greatly increase their degree of senior management attention, measure performance of officials charged with security responsibility and improve security education and awareness, fully integrate security into their capital planning investment and control process and enterprise architecture, ensure that contractor services are adequately secured, and improve the ability to detect, report and share information on incidents and vulnerabilities.

As we look at the future or what we call the "to be" state of Federal security, we believe it is one of the active measures that will continue to anticipate and respond to future needs. The future vi-

sion of Federal security incorporates active measures and we have to be able to both prepare and defend against attacks where preemption is not possible so that we know how our own information systems survive attacks when defenses fail.

Such a state is somewhere off in the future, however, and such a number of fundamental management and program reforms are needed to support it. Particularly, we need to complete the development of governmentwide and agency-specific architectures within which business processes have been unified and simplified, and get rid of unnecessary duplication so we not only promote common ways to conduct government business, it will permit common protection regimes and simplified security approaches.

The "to be" state also requires much in the way of using automated security tools that reduce the need for human intervention and reduce human error and resource requirements. The "to be" state of anticipating threats will also require something that is woefully lacking today, rapid and in-depth threat analysis. Today's analysis products largely consist of consolidated reports of what is happening or what has already occurred. That is not good enough. We must improve the development, quality and wide distribution of effective threat analysis and response regimes.

OMB is pursuing a five part approach to improved government security which includes items such as business cases, capital planning, project matrix analysis, which I have spoken about before, annual agency security reports and corrective action plans that reflect priorities. All efforts must come together to clear us clear audit trails that link the needs, corrective action plans and spending priorities including business cases. More detail on that is in my prepared statement.

Through this five part approach, we are building toward a "to be" state and believe within 18 months we will have demonstrably improved performance and results in agency security programs. We give some of the details of that in my prepared statement. That includes using security performance measures that identify the gaps and set priorities within each agency and form agency and OMB budget decisions and assist in preparing the President's budget.

We are also identifying opportunities to reduce or eliminate unnecessary duplication of security effort among agencies making certain practices more uniform and consolidating programs and operations to increase performance while reducing costs. Among the candidates for consolidating greater uniformity are consolidating the security curriculum as well as the actual conduct of training and education and awareness for Federal employees; improving incident handling, information sharing, software patch identification and distribution; improving methods for grading or designating the level of risk, assigning core security requirements for operations, assets and the same risk level, unifying and simplifying requirements for and implementation of contingency planning and continuity of operations, improving security and the acquisition of products and services, very similar to some of the concepts outlined in Congressman Davis' bill.

While many security requirements within the Government are similar, many are distinctly different. Therefore we must be careful and resist overly simplistic attempts to standardize management,

operational and technical security controls. Security controls must be built to the specifications of the programs, not programs built to security initiatives.

NIST continues to play a critical role in supporting OMB and assisting agencies in improving their security performance and there are details in my prepared testimony.

I want to finish up by talking about the specific stats associated with the OMB chaired executive branch Information Systems Security Committee which is one of the components of the President's Critical Infrastructure Board. I mentioned this in my statement at the March hearing.

Last month, we held our first meeting of the committee and have begun work on the following four issues, and details are in my prepared testimony: grading risks; uniform security practices, including acquisition of products and services; review of current policy standards and guidance.

Future security reporting will drive the performance improvements not simply tallying numbers. As GAO, OMB and others recognize, today's information security world demands each agency employ a continuing process of risk-management that keeps pace with rapidly evolving threats and vulnerabilities. So too, OMB's oversight process must keep up with the changes in status. A conventional view is the comparison should show security weaknesses have been reduced and no new ones have cropped up. That, we believe, is the old way of thinking.

Identifying more weaknesses is not necessarily a reflection of performance. Reaching the "to be" state I described earlier demands more deeply and more often into programs and systems to find problems as the vulnerabilities arise and before they can be exploited. The more you look, the more you find.

In conclusion, we have developed a strategy to measure program performance and drive improvements by an order of magnitude. Some of what is needed involves technology, much more involves integrating security into project development and management decisionmaking. At this point in time, new standards and technology, while impacting little in improving security performance, must be first addressed and correct management weaknesses.

We look forward to working with the committee and Congressman Davis as the bill moves forward through the process.

[The prepared statement of Mr. Forman follows:]

STATEMENT OF
MARK A. FORMAN
ASSOCIATE DIRECTOR FOR INFORMATION
TECHNOLOGY AND ELECTRONIC GOVERNMENT
OFFICE OF MANAGEMENT AND BUDGET
BEFORE THE
COMMITTEE ON GOVERNMENT REFORM
SUBCOMMITTEE ON GOVERNMENT EFFICIENCY,
FINANCIAL MANAGEMENT, AND INTERGOVERNMENTAL RELATIONS AND
THE SUBCOMMITTEE ON TECHNOLOGY AND PROCUREMENT POLICY
U.S. HOUSE OF REPRESENTATIVES
May 2, 2002

Good morning Mr. Chairman and members of the Committee. Thank you for inviting me here today to discuss the Federal information systems security and the Federal Information Security Management Act. I will discuss these in the context of the current state of Federal security and our vision for the future.

Before I get into the substance of my testimony, I need to make sure that the Subcommittee understands that I do not serve in a confirmed position within the Office of Management and Budget (OMB). As a general policy, OMB does not usually send officials in non-confirmed political positions to testify before Congress. However, because of the importance of the issue and the fact that OMB does not yet have a confirmed Deputy Director for Management, the OMB Director decided it was in the best interest of the Administration to have me appear on his behalf as a witness for this hearing.

I know you would like to hear today about our specific views on the Federal Information Security Management Act. While we at OMB and other Administration officials have discussed components of the Act with your staff, we are still developing an Administration position on the bill. We look forward to working with you as the bill moves through the legislative process. We are also working with your Senate colleagues on S.803 the "Electronic Government Act of 2002." As you know that bill simply reauthorizes the Government Information Security Reform Act (Security Act) by lifting the November 2002 sunset date on the statute.

As you know, the President has given a high priority to the security of government assets as well as to

improving the overall management performance of Executive agencies. These priorities are interrelated. As I discussed this past March before the Committee, our review of agency security programs found that most security problems within the government are fundamentally management issues. We are tracking progress on both issues through the use of the Executive Branch Scorecard for the President's Management Agenda. This Scorecard tracks agency improvement in five government-wide issue areas and assigns a red, yellow, or green score. One of the five areas, expanding electronic government, directly incorporates security. This means that if an agency does not meet the IT security criterion it will not achieve a green score regardless of their performance under the other e-gov criteria.

Vision for Federal Security

Our vision for Federal government security is an order of magnitude improvement to support government programs and enable a successful expansion of e-government. Security -- providing the necessary degree of confidentiality, availability, integrity, reliability for data and systems and ensuring the authenticity of transactions -- is integral to successful e-government.

The "As Is" State of Federal Security

As OMB reported in our February 13, 2001, security benchmark report to Congress on Government Information Security Reform, the "as is" state of security across the Federal enterprise is poor. We reported on six common fundamental government-wide weaknesses, as well as agency specific gaps. These weaknesses are pervasive and many exist within both the national security community and the larger non-national security community of Federal agencies.

We found that agencies must greatly increase their degree of senior management attention, measure the performance of officials charged with security responsibilities, improve security education and awareness, fully integrate security into the capital planning and investment control process and enterprise architecture, ensure that contractor services are adequately secure, and improve the ability to detect, report, and share information on incidents and vulnerabilities.

Through the use of OMB's authorities under existing law, most particularly the Paperwork Reduction Act of 1995, the Clinger-Cohen Act of 1996, and the Government Information Security Reform Act of 2000, we are using the capital planning and investment control and the budget process to drive performance improvements in all of the problem areas that we identified.

The "To Be" State of Federal Security

The "to be" state of Federal security is one of active measures to anticipate future threats and vulnerabilities, preempt them where we can, prepare and defend against them where preemption is not possible, and survive attacks when defenses fail. Such a state is some years off however and a number of fundamental management and program reforms are needed to support the consistent and increased use of automated tools to manage threats. Many of these reforms are envisioned in the e-government initiatives and are outside of the control of security programs. Particularly, we need to complete the development of agency and government-wide architectures within which business processes have been unified and simplified and unnecessary duplication removed. This will not only promote common ways to conduct government business, it will permit common protection regimes and simplified security approaches.

The "to be" state also requires much in the way of using and improving existing automated security tools and developing new ones that reduce the need for human intervention and reduce human error and resource requirements. These are force multipliers for security and will assist in addressing some of the technology induced security problems. They will not however address all security problems as security is ultimately a management issue and technology demands the management commitment to sustain the use of technology.

The "to be" state will also include centralized and simplified ways to train Federal employees and to automate the retrieval and installation of patches and hot fixes for technology problems much in the way individual systems owners can do today. Again however, such a state depends first upon a more uniform business and technical architecture than currently exists.

Improved Incident Handling and Reporting and Cross-Government Data Sharing

The "to be" state of anticipating threats will also require something that is woefully lacking today, in depth threat analysis. Today's analysis products consist largely of consolidated reports of what is happening or what has already occurred. That is not good enough. We must improve the development, quality, and wide distribution of threat analysis performed by government and industry leaders. Only in this way will agencies be capable of anticipating and preempting threats and vulnerabilities versus reacting to incidents after they have begun. This will not occur overnight and wisely spent research and development funding will be crucial to success.

Near and Mid-Term Steps to Achieve the "To Be" State

Security Improvements at the Agency Level

We are building towards the "to be" state and within 18 months, we will demonstrably improve the performance and results of agency security programs through:

1) Completing the integration of security into the agency's enterprise architecture and capital planning and investments control process to ensure that agencies make better decisions when investing in information technology and that the adequate level of business enabling and cost effective security is built into and funded over the life cycle of all IT projects,
2) Improving security management at each agency and integrating it into the agency's overall management structure and processes thus permitting each agency to move from today's reactive security posture to one of continuous risk management including the use of automated tools to actively look for, anticipate, and counteract threats and vulnerabilities before they are employed or exploited,
3) Ensuring that each department and agency maintains a department-wide program which actively oversees and verifies improved security performance in all components,
4) Measuring agency and component security performance and progress through reporting requirements under the Government Information Security Reform Act and through

use of the President's Management Agenda Scorecard, and

5) Using security performance measurements to identify performance gaps and set priorities within each agency, inform agency and OMB budget decisions, and assist in preparing the President's budget.

Security Improvements at the Federal Enterprise Level

We are also seeking to improve the federal government's internal effectiveness and efficiency by simplifying and unifying security to facilitate programs and interoperability among Federal agencies and with State and local governments, industry, academia, and the public.

Many agencies perform similar business operations, especially internal management operations. The security requirements for such operations are also similar. Potential values in unifying and simplifying security include reduction or stabilization of staff resources, operational effectiveness, and stabilized spending.

Using an e-government-like approach, we are identifying opportunities for reducing or eliminating unnecessary duplication of security effort among agencies, making certain practices more uniform, and consolidating programs and operations to increase performance while reducing costs. Among the candidates for consolidation or greater uniformity are:

1) Consolidating security curriculum development as well as the actual conduct of training, education, and awareness for Federal employees. This will reduce unnecessary duplication of individual agency training infrastructures,
2) Improving incident handling, information sharing, and software patch identification and distribution. Centralizing access to and implementation of security patches will be more cost effective and improve agency performance,
3) Improving methods for grading or designating the level of risk to agency operations and assets. Developing a uniform methodology for use by all agencies will promote a common understanding of risk levels and facilitate interoperability and information sharing,

4) Assigning core security requirements for operations and assets at the same risk level. Many agency operations and systems are the same and so to are many of their security requirements,
5) Unifying and simplifying requirements for and implementation of contingency planning and continuity of operations for agency communications and data networks. All critical Federal operations require the capability to continue or quickly restore functions and the methods to do so and implementation should be consistent across the Federal enterprise,
6) Improving the acquisition of products and services. In this two part effort, we will ensure that as law requires, all outsourced Federal operations be secured in the same manner as in-house operations and leverage the combined purchasing power of the Federal government and its industry partners to provide an incentive for industry to develop more reliable and secure products for all consumers.

A Cautionary Note - For Security, One Size Does Not Fit All

While many security requirements within the government are similar, many are distinctly different. We must be careful and resist overly simplistic attempts to standardize management, operational, and technical security controls in a non-standardized world. Thus, security controls must be built to the specifications of the program, not vice versa.

Attempting a one size fits all security approach is the fundamental flaw in past and some present attempts to standardize security. This is especially true when we try to apply national security requirements to non-national security programs where the vast majority of programs demand interoperability with industry, academia, and the public. Certainly, many of the needs are similar, and we must share approaches where we can, but the differences are far greater and require greater flexibility.

We have many historic examples of what happens when security is employed that is incompatible with the business needs. These examples exist within both the national security community and the non-national security community. Some of these are contemporary history, playing out before us today.

Draconian and costly new security controls are often developed and employed following a significant security breach while an organization still feels the sting of embarrassment. These controls may work for a while, but are soon recognized as such an impediment to the mission that restrictions are relaxed, waived, or worse, ignored and worked around. As the sting subsides, further relaxation and waivers occur and the organization often finds itself back to the beginning point - no security. The cycle repeats itself.

Our approach is to fully integrate risk-based and cost effective security into the business processes and agency decision-making and thus avoid wild swings in security performance.

A Continued Strong Role for NIST is Essential to Improving Government-wide Security

NIST continues to play a critical role in supporting OMB and in assisting the agencies improve their security performance by developing new and updated technical guidance and detailed procedural security guidelines. They have recently either finalized or issued for public comment guidance on risks involving broadband telework and securing web and electronic mail servers. They will soon release for comment guidance regarding the security of wireless networks - an increasingly popular technology whose use is not without risk. Soon, NIST will release the automated version of their security self-assessment tool that most agencies used last year (including some within the national security community) to conduct their security reviews for reporting to OMB.

Among the most valuable of NIST's many abilities is fostering an open process (working with agencies, industry, and academia) that ensures that risks are objectively assessed and security guidance includes an understanding of the real world needs of agency program operations.

Working with NIST, one of the ways OMB is assisting the agencies is through a review of all current security policies, standards, guidance, and guidelines to identify gaps in coverage and effectiveness. Where gaps are found we will close them, where confusion or uncertainty exists,

we will clarify and simplify, and where more detail is necessary, we will provide it.

We began this gap analysis in April using the OMB-chaired Committee on Executive Branch Information Systems Security. This committee, which was established by E.O. 13231, "Critical Infrastructure Protection in the Information Age," is comprised of Chief Information Officers, Chief Financial Officers, Procurement Executives, Inspectors General, operational program officials (business lines), budget officials, human resource officials, security program managers, representatives from the national security community, law enforcement officials, and small agency representatives - all communities affected by security.

The policy gap analysis, as with all issues reviewed by this committee, will assess the performance benefits and costs of current or proposed policies in terms of whether they specifically: 1) are consistent with the President's Management Agenda and electronic government initiatives; 2) assist or impede agency business operations including introducing unintended negative consequences to program operations; 3) are workable for small agencies; 4) complicate or simplify interoperability across agencies, with industry, and other organizations; 5) complicate or simplify implementation and compliance; 6) complicate or simplify procurement and acquisition decisions; 7) increase or reduce privacy; 8) assist or impede Homeland Security and law enforcement efforts.

Federal Enterprise Architecture and Inter-Relationships

To ensure complete and adequate security coverage, we are also identifying within the individual agencies, among multiple agencies, and across the government enterprise and various lines of government business, the key operations and assets of the government and their inter-relationships. This will permit us to better identify security needs including contingency planning for those key lines of government business. It will also help us eliminate inconsistent security approaches across interrelated operations -- identifying the vault door on a shack.

Through the development of agency enterprise architectures and the use of Project Matrix we are collecting this information now. While the current process

captures much in the way of cross-organizational relationships, we have also allocated resources for a horizontal, cross government review by business line to identify any gaps in the agency-by-agency review. As part of this process, through the use of simulation models, we will evaluate the impact of threats on cross agency processes including continuity of business operations and data sharing.

Future Security Reporting Will Drive Performance Improvements, Not Simply Tally Numbers

As GAO, OMB and others recognize, today's information technology world demands that each agency employ a continuing process of risk management that keeps pace with the rapidly evolving threats and vulnerabilities. So too, OMB's oversight process must keep up with the changes in the status of agency programs.

Last year, as the Security Act required, we collected and provided to Congress a retrospective look at the state of each agency's security program -- a security baseline. This year we will collect much of the same data and will compare it to last year's baseline. The conventional view is that the comparison should show that security weaknesses have been reduced and no new ones have cropped up. But that is the old way of thinking -- identify last year's problems and wait until next year to see if the number has gone down.

This spring we are discussing with each of the large agencies the quality of last year's reporting and their plans to correct weaknesses identified in those reports. We have emphasized that we expect that the number of reported weaknesses to increase as they improve the quality of their self-assessment programs and reporting. More identified weaknesses is not necessarily a reflection of poor performance -- the more you look, the more you find - and OMB will not penalize agencies for finding more problems, provided of course they are taking appropriate measures to correct them in a timely manner and avoid recurrence.

OMB and NIST are also meeting with small and independent agencies either individually or collectively to ensure that they understand their responsibilities and are taking steps to fulfill them. We will look for ways that

they can partner with each other or work with larger agencies to assist them in achieving security performance improvements.

Reaching the "to be" state I described earlier demands digging more deeply and more often into program and systems to find and fix problems before they are exploited or an inspector finds them. Thus we are using the agency corrective action plans to drive this continuing process and are a key element for OMB oversight.

These corrective action plans must be the authoritative agency management tool to identify and manage the closing of agency security performance gaps. They must reflect all security weaknesses within an agency including its components and effective plans are iterative and do not have a specific beginning or end point. As old problems are corrected, they are removed. As new ones are found, they are added on.

What does a good plan look like? In addition to being a living document that catalogs problems as they are found, for a large agency, a comprehensive plan will consist of scores or hundreds of pages comprising hundreds or thousands of weaknesses. These weaknesses vary in detail from broad headquarters program level issues to minute technical problems within individual systems located in remote field activities. Such a plan would also include the names of agency employees that are being held accountable for correcting individual security weaknesses.

OMB's guidance prescribes a level of detail that enables agency management and OMB to manage and oversee security and inform the budget process. To meet OMB requirements, agency plans must include subjective and predecisional data to support a free and frank discussion between each agency and OMB. This data includes the agency's views of future resource requirements, the proposed source of those resources, and relative priorities for corrective actions and resources. In developing the President's budget, OMB must then view the security data together with agency budget submissions in the larger context of all government programs and priorities. Inaccurate assumptions invariably result from viewing predecisional data out of the larger context.

Many agencies have recognized that effective security management across a large organization requires that they collect and manage even more data than the minimum requested by OMB and they have or are developing complex databases that track this data.

Congress has an Essential Oversight Role

Congress and GAO are important strategic partners in our efforts to actively oversee government-wide security performance. We must all work together to move from the "as is" state to the "to be" state.

OMB agrees that some, perhaps most, of the data in the agencies' corrective action plans should be made available to Congress and we are modifying our guidance to the agencies to accommodate that goal.

OMB agrees that Congress has an important oversight role and will work toward an acceptable solution as quickly as possible. The challenge at this point involves identifying the proper level of detail, how to cull it from the predecisional data with which it is intertwined, and setting a reasonable schedule to provide it. We are addressing Congressional access needs in our guidance for the next agency submission of full corrective action plans next Fall.

Conclusion

As I told the Committee last March, we have found the current state of government security to be poor. We have identified about 200 agency information technology projects that are at risk due to poor security and there are probably as many more that could be on the list. Our goal is to find ways to assist the agencies in bringing them up to an acceptable level of performance.

We have developed a strategy to measure program performance and drive improvements by an order of magnitude. Some of what is needed involves technology, but much more involves integrating security into project development and management decision making. At this point in time, new standards or technologies will have little impact on improving security performance unless we first address and correct management weaknesses.

Mr. HORN. We thank you for that and we will have a number of questions when we finish the panel.

We next have Daniel G. Wolf, Director, Information Assurance Directorate, National Security Agency. He has had responsibility for the various information situations and strategies to protect the defense information infrastructure and as appropriate, the national information infrastructure. He spent about 33 years in this type of analytic work and has received numerous awards for his many contributions in defense intelligence communities. We are delighted to have you here. We have had great cooperation from the National Security Agency and we appreciate the tough job he has and they have. We are glad to have you here. Mr. Wolf.

Mr. WOLF. My name is Dan Wolf and I am NSA's Information Assurance Director. I appreciate the opportunity to be here today to talk about information technology security as your subcommittee considers H.R. 3844.

My organization is responsible for providing IA technologies, services, processes and policies that protect national security information systems throughout DOD, the intelligence community and related law enforcement agencies. While some may suggest that NSA's perspective is too narrow because we focus on national security systems, I would like to note NSA has been in the business of protecting information systems from attack and exploitation since 1953.

During NSA's nearly 50 years of producing not only policy but also in the hard work of developing security products and services to implement these policies, we have learned, and I believe we agree with many members of this committee that successful information security demands aggressive management oversight, extensive sharing of best practices and a bedrock foundation of proven security standards.

While I am not in a position to express the administration's view of H.R. 3844, I thought it might be helpful if I shared NSA's technical experience in these matters with you. There are a number of areas in H.R. 3844 where we believe improvements can be made based on our experience. My written testimony goes into much more detail but I would like to briefly highlight four areas.

The first area is defining and identifying national security and mission critical systems. We suggest that the proposed definition for identifying national security systems in H.R. 3844 might add more confusion to an already complex process. We have also learned by analysis of dependence between computer systems during the Y2K crisis, that there are many similarities found in identifying and protecting mission critical systems and national security systems. Therefore, we suggest that you consider keeping the original GISRA definition of national security systems.

In a related matter, the provision that directs NIST to develop guidelines for identifying an information system as a national security system is unnecessary because the national security system is already defined in the existing laws.

The second area is risk assessments and system engineer connection management processes. There are many references to a risk assessment process in H.R. 3844. It has been our experience that useful risk assessments are extremely difficult to complete and

maintain. This problem gets especially dangerous when you consider that although these systems are assessed for risk independently, they soon become interconnected. We have consistently found one organization's risk calculations and assumptions will be very different from another unless the process of performing the risk assessment is exceptionally well specified and managed.

We suggest that a standard method for performing risk assessments be developed for use throughout the Federal Government. It must describe not only the assessment process but also define standard methods for characterizing threats, defining potential mission failures and include a process for ensuring that these baseline risk assessments are periodically reevaluated, especially as changes are made in connectivity. The quality of risk assessments for our interconnected systems must not be left to chance or independent decisions. Otherwise, the weakest link in the chain will fail.

Third, coordinating incident detection and consequence management, the defense of Federal and DOD networks against cyber attacks requires a robust and time sensitive defense in-depth approach. NSA's National Security Incidence Response Center provides real-time reporting of cyber attack incidences. Through around the clock, 7-day-a-week operation, NSIRC provides DOD, the intelligence community and the Federal law offices with information valuable in identifying and encountering cyber attacks. NSA has established a trusted relationship with the Fed CIRC. Moreover, we have similar relations with the National Infrastructure Protection Center and the NIPC and the Department of Defense's Incidence Center, the DODCERT. We believe that adding a new Federal Incident Management Center as described in the proposed legislation would add unnecessary redundancy and decrease both the efficiency and effectiveness of our existing processes.

Fourth, sharing vulnerability information, the technology we used today throughout the Government and the private sector is a veritable monoculture. For example, this means that knowledge of vulnerability discovered in a system at the Labor Department could be used by an adversary to attack the computer in the Defense Department. While we agree it is extremely important for all Federal departments to share vulnerability information, we also believe this information must be disseminated only through consideration regarding the consequences, not just to an organization's internal systems but the consequences to all Government systems is vulnerability becomes widely known.

I would like to thank the members of both subcommittees for your consistently strong interest and attention to this vital area. Your leadership is providing a public service by raising the issue of the serious security challenges we are all facing in the age of interconnected and interdependent networks.

This concludes my testimony. I would be happy to answer any questions.

[The prepared statement of Mr. Wolf follows:]

Statement by

Mr. Daniel G. Wolf

Information Assurance Director

National Security Agency

Before the

House Committee On Government Reform

Subcommittee on

Government Efficiency, Financial Management and

Intergovernmental Relations

and the

Subcommittee for

Technology and Procurement Policy

Joint Hearing on

H.R. 3844: The Federal Information Security Reform Act of 2002

2 May 2002

For Official Use Only
Until Released by the
U.S. House of Representatives
Committee on Government Reform

Good morning Chairman Horn, Chairman Davis, and distinguished members of both Subcommittees—thank you for inviting the National Security Agency to provide comments on H.R. 3844, "The Federal Information Security Reform Act of 2002".

I also would like to thank the Members of both Subcommittees for their consistently strong interest and attention to this vital area over the past few years. Your leadership is providing a genuine public service in raising the visibility of the serious security challenges we all face in an age of interconnected, inter-dependent digital networks.

My name is Daniel Wolf and I am NSA's Information Assurance Director. My comments to H.R. 3844, "The Federal Information Security Management Act of 2002," are provided from NSA's perspective. NSA's Information Assurance Directorate is responsible for providing information assurance technologies, services, processes and policies that protect national security information systems. While some may suggest that NSA's perspective is too narrow due to our focus on the stringent requirements of national security systems, I would like to note that NSA's Information Assurance Directorate and its predecessor organizations have had policymaking and implementation responsibility regarding the protection of national security telecommunications and information processing systems across the Executive Branch since 1953.

During our nearly 50 years of producing not only security policies but also in the hard work of deploying security products and services that implement those policies, we have learned—and in this we agree with many members of this committee—that successful information security demands aggressive management oversight, extensive sharing of best practices, and a bedrock foundation of proven security standards. Accordingly, the National Security Agency generally supports passage of the Federal Information Security Management Act of 2002. While we believe that the proposed legislation provides the necessary next step in the continuing process of enhancing the protection afforded critical federal information systems, we offer a number of suggestions for your consideration for improving the act in the following areas:

1. Defining and identifying national security and mission critical systems
2. Risk assessment and system interconnection management
3. Conducting annual evaluations
4. Coordinating policies
5. Coordinating incident detection and consequences management
6. Sharing vulnerability information

I believe it is useful to provide a brief description of the responsibilities and scope of NSA in the area of Information Assurance (IA) and NSA's policymaking functions and authorities before providing additional details regarding the specific suggestions we offer to H.R. 3844.

NSA Information Assurance Background

When I began working at NSA some 33 years ago, the "security" business we were in was called Communications Security, or COMSEC. It dealt almost exclusively with providing protection for classified information against disclosure to unauthorized parties when that information was being transmitted or broadcasted from point to point. We accomplished this by building the most secure "black boxes" that could be made, employing high-grade encryption to protect the information. In the late 1970s, and especially in the early 1980s with the advent of the personal computer, a new discipline we called Computer Security, or COMPUSEC, developed. It was still focused on protecting information from unauthorized disclosure, but brought with it some additional challenges and threats, e.g., the injection of malicious code, or the theft of large amounts of data on magnetic media. With the rapid convergence of communications and computing technologies, we soon realized that dealing separately with COMSEC on the one hand, and COMPUSEC on the other, was no longer feasible, and so the business we were in became a blend of the two, which we called Information Systems Security, or

INFOSEC. The fundamental thrust of INFOSEC continued to be providing protection against unauthorized disclosure, or **confidentiality**, but it was no longer the exclusive point of interest. The biggest change came about when these computer systems started to be interconnected into local and wide area networks, and eventually to Internet Protocol Networks, both classified and unclassified. We realized that in addition to confidentiality, we needed to provide protection against unauthorized modification of information, or data **integrity**. We also needed to protect against denial-of-service attacks and to ensure data **availability**. Positive identification, or authentication, of parties to an electronic transaction had been an important security feature since the earliest days of COMSEC, but with the emergence of large computer networks data and transaction **authenticity** became an even more important and challenging requirement. Finally, in many types of network transactions it became very important that parties to a transaction not deny their participation, so that data or transaction **non-repudiation** joined the growing list of security services often needed on networks. Because the term "security" had been so closely associated, for so long, with providing confidentiality to information, within the Department of Defense we adopted the terms **Information Assurance**, or IA, to encompass the five security services of confidentiality, integrity, availability, authenticity and non-repudiation. I should emphasize here that not every IA application requires all five security services, although most IA applications for national security systems – and all applications involving classified information – continue to require high levels of confidentiality.

Another point worth noting is that there is an important dimension of Information Assurance that is operational in nature and often time-sensitive. Much of the work of Information Assurance in providing an appropriate mix of security services is not operational or time-sensitive, i.e., education and training, threat and vulnerability analysis, research and development, assessments and evaluations, and tool development and deployment. In an age of constant probes and attacks of on-line networks, however, an increasingly important element of protection deals with operational responsiveness in terms of **detecting** and **reacting** to these time-sensitive events. This defensive operational capability is closely allied and synergistic with traditional Information

Assurance activities, but in recognition of its operational nature is generally described as **Defensive Information Operations**, or DIO.

NSA's responsibilities and authorities in the area of information assurance are specified in or derived from a variety of Public Laws, Executive Orders, Presidential Directives, and Department of Defense Instructions and Directives. Chief among them is the July 1990 "National Policy for Security of National Security Telecommunications and Information Systems" (NSD-42).

This National Security Directive designates the Secretary of Defense as the Executive Agent for National Security Telecommunications and Information Systems Security (NSTISS), and further designates the Director of NSA as the "National Manager" for NSTISS. The Directive assigns the Director, NSA, broad responsibilities for the security of information systems processing classified or unclassified national security information, including:

- Evaluating systems vulnerabilities
- Acting as the focal point for cryptography and Information Systems Security
- Conducting research and development in this area
- Reviewing and approving standards
- Conducting foreign liaison
- Operating printing and fabrication facilities
- Assessing overall security posture
- Prescribing minimum standards for cryptographic materials

- Contracting for information security products provided to other Departments and Agencies

- Coordinating with the National Institute of Standards and Technology (NIST); providing NIST with technical advice and assistance

NSD-42, in addition to defining NSA's responsibilities for information systems security, established the Executive Branch's formal policymaking mechanism for national security information systems security. This body, the National Security Telecommunications and Information Systems Security Committee (NSTISSC), is comprised of 21 Members from Executive Branch Departments and Agencies. Although there are 11 official observers, over 50 government organizations regularly participate in various NSTISSC activities, subcommittees, and working groups.

The President redesignated the NSTISSC as the Committee on National Security Systems (CNSS) by signing Executive Order 13231, Critical Infrastructure Protection in the Information Age, on October 16, 2001. The CNSS was also made a standing committee of the President's Critical Infrastructure Protection Board.

The incumbent Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD/C3I) chairs the CNSS. The Committee performs a number of important functions, including approving the release of information systems security equipment and information to foreign governments and organizations – usually for military interoperability purposes – through a careful assessment and voting process. The Committee's primary function, however, is to issue, implement, and maintain Information Assurance policies, directives, instructions, and advisory memoranda.

The CNSS currently has over 100 of these policy issuances in effect, and many of them directly relate to the important details of achieving assurance in classified and national security information systems. It is important to note that the three predecessor organizations of the NSTISSC (United States Communications Security Board, National Communications Security Committee, and National Telecommunications and

Information Systems Security Committee), going back to 1953, had policymaking responsibility for national systems across the Executive Branch.

NSA has several key roles in the CNSS. As noted above, the Director of NSA is the "National Manager" for National Security Telecommunications and Information Systems Security, and as such signs the CNSS' issuances. NSA also provides day-to-day support to and management of CNSS activities by providing a senior official to act as the organization's Executive Secretary. Most importantly, NSA provides a permanent Secretariat of full-time staff personnel, facilities, and other necessary support such as funding, printing and distributing documents, sponsoring a Web site, managing voting processes, maintaining official records, developing policy and doctrine proposals, and organizing committee, subcommittee, and working group meetings, as well as an annual conference.

Specific Comments to H.R. 3844

1. Defining and identifying national security and mission critical systems

We suggest that the modified definition found in the amended Section 3532 may possibly add confusion to the already complex process of identifying 'national security systems' by adding another source rather than citing an existing source for defining the term as was done in the original GISRA language. We also believe that that there are significant parallels found in identifying, characterizing and protecting mission critical systems and national security systems as we learned by our collective efforts to determine critical dependencies between computer systems during the Y2K crisis. Therefore we suggest returning to the language as specified in the original GI SRA Section 3532 (b)(2).

In a related matter, we suggest that the 'guidelines for identifying an information system as a national security system' in the amended Section 20 (b)(3) of the National Institutes of Standards and Technology Act (15 U.S.C. 278g-3) be changed. We believe that the Director, NSA, as National Manager of National Security Telecommunications and Information Systems Security should be assigned the responsibility for developing

specific guidance for identifying national security systems. We further suggest that the CNSS is the appropriate forum to coordinate this guidance and, after approval by the committee, to issue it.

2. Risk assessments and system interconnection management processes

There are a number of references throughout H.R. 3844 where the concepts of risk assessment and risk management are included. It has been our experience that comprehensive and useful risk assessments are extremely difficult to initially complete and even harder to maintain throughout a system's lifetime. This problem gets potentially dangerous when you consider that systems that are independently assessed for risk are soon interconnected. One organization's calculation for acceptable risk may be very different from another's. But in the richly interconnected world of federal systems—a risk taken by one system is ultimately borne by all the others.

We suggest that the committee consider assigning a high priority to the development of a comprehensive standard for federal system risk assessment and management. The standard should describe—not only the assessment process and documentation requirements—but also include standard methods for characterizing adversarial threats and capabilities, determining categories for mission impact and offer a method for ensuring that the assumptions used in the risk assessment are adjusted as appropriate over time.

A risk assessment—in an interconnected world—cannot be simply completed at the time a system is certified and then filed away. It must become a living document, a sort of trusted calling card that is used when two systems are negotiating their interconnection. The quality of the risk assumptions, calculations and decision thresholds cannot be safely left to chance or independent decisions. There must also be a common method throughout the federal government for managing system interconnection based on a standardized approach to risk assessment. Otherwise, the weakest link in the chain will most certainly break.

3. Conducting annual evaluations

We suggest that Section 3535(b) as amended by HR 3844, mandating that annual evaluations for each agency with an Inspector General be performed by the Inspector General or by an independent external auditor, as determined by the Inspector General be reconsidered. It is our experience that the necessary technical competence to either conduct the evaluation or to specify the terms for an information system security effectiveness assessment may not always reside with the Inspector General. We recommend that subsection (b) be deleted, and that it be replaced by subsection (c), amended to provide that in all cases the department or agency head shall determine what internal or external body will perform an annual evaluation.

4. Coordinating policies

Section 3533(a)(3) encourages the coordinated development of standards and guidelines with agencies and offices operating national security systems. We suggest that additional efficiencies could be gained by requiring the Director in cooperation with the CNSS, to annually conduct a complete review of all related 'national security systems' policies, practices, guidelines, and standards to identify and report on those that are most relevant and prioritize a complementary publication schedule.

5. Coordinating incident detection and consequences management

The Federal Information Security Incident Center described in Section 3536 has confused us. We offer no comment if this section is intended to provide authorizing language for the existing Federal Computer Incident Response Center (FedCIRC) operated by the General Services Administration. However, if this section were intended to propose an additional federal incident management center then we would respectfully ask the committee to reconsider.

The defense of both the National Information Infrastructure (NII) and the Defense Information Infrastructure (DII) requires a robust and time-sensitive Defense-in-Depth approach. To help meet this challenge, NSA's National Security Incident Response Center (NSIRC) provides near real-time reporting of cyber attack incidents, forensic

cyber attack analysis, and threat reporting relevant to information systems. Through round-the-clock, seven-days-a-week operations, the NSIRC provides the Departments of Defense, the Intelligence Community, Federal Law Enforcement and other Government organizations with information valuable in assessing current threats or defining recent cyber intrusions.

The NSIRC at NSA has established a trusted relationship and a proven set of analytical and reporting processes with the FedCIRC. Moreover, we have similar relationships with the National Infrastructure Protection Center (NIPC) and the Department of Defense's Incident Center (DODCERT) that were created over the past 3 years.

We believe that adding a new federal incident management center would add unnecessary redundancy and decrease both the efficiency and effectiveness of the community and the NSIRC.

6. Sharing vulnerability information

We agree that it is extremely important for all federal agencies and departments to develop effective procedures for the timely dissemination of information system security vulnerability information. However, we also believe that this information must be controlled and disseminated with the utmost care and only after thorough consideration regarding the possible consequences not just to an organization's local systems—but to all related federal systems.

Today's information technology is a veritable monoculture. There is very little diversity in the underlying technology and therefore the security vulnerabilities found in national security systems as compared with other federal systems. Section 3535(c)(2) of the proposed amendment requires appropriate protection of information security vulnerability information. However, we would encourage the committee to consider adding language that provides for the appropriate protection of this type of information regardless of the system from which it was derived.

This concludes my testimony and Statement for the Record. Once again, I thank you both, and the Members of these Subcommittees for the opportunity to comment on H.R. 3844. I will be pleased to answer any questions you may have.

Mr. HORN. Thank you.

Next is a person well known to this subcommittee and the Congress, Mr. Benjamin Wu, Deputy Under Secretary of Commerce for Technology Administration, Department of Commerce. He was very helpful to us in our Y2K computer problems and worked very closely with Representative Morella of Maryland in her role on the Science Committee as well as in Government Reform. Nice to see you again.

Mr. WU. Thank you, Chairman Horn, and good morning. Good morning to you, Mr. Davis and also Ranking Member Schakowsky.

On behalf of the Department of Commerce's Technology Administration and its National Institute of Standards and Technology, I want to share with you our views on Congressman Davis' bill, H.R. 3844.

Let me first commend you, Mr. Chairman, and the entire subcommittee for continuing to focus on the critical issue of cyber security in the Federal Government. Today's hearing will once again remind Federal agencies that cyber security must be addressed in a comprehensive manner and on a continuing basis.

As you mentioned, I had the privilege and the pleasure of working with you, Chairman Horn, and also Chairman Davis, as we successfully battled the Y2K computer problem which some have drawn parallels to the issue of computer security. With Y2K as you well know, we knew who the enemy was, we knew how it was going to strike, we knew when it was going to attack. We don't have that luxury with computer security. That is why it is important that we continue to focus on Federal efforts on computer security and I am very proud that NIST plays an important cyber security role for our Nation.

We have specific statutory responsibilities for Federal agencies under the Computer Security Act of 1987 and also its follow on legislation, including GISA. NIST has been tasked by Congress to develop standards and guidelines to assist the Federal Government in protection of sensitive, unclassified systems. These responsibilities supplement NIST's broader mission of strengthening the U.S. economy, including proving the competitiveness of America's information technology industry.

In support of this mission, NIST conducts standards and technology work to help industry produce more secure, yet cost effective products which we believe will enhance competitiveness in the marketplace. Having more secure products available in the marketplace will also benefit Federal agencies because they principally use commercial products that construct and secure their systems.

The Computer Security Division in our Information Technology Laboratory is the focal point of our cyber security program. The Computer Security Division focuses on a few key areas: photography standards and applications, security research, security management, and security testing. In previous testimony before this committee on March 6, the Director of NIST, Arden Bement, provided you with a broad review of current NIST activities undertaken to fulfill our important cyber security responsibilities, so it is not necessary to repeat to you what NIST is doing now but I do want to discuss with you what NIST would be asked to do if H.R. 3844 was enacted, as introduced, and offer some comments.

Under FISMA, NIST would be tasked with a number of responsibilities ranging from developing IT standards and guidelines, developing security standards and guidelines, consulting with other Federal agencies, providing assistance to agencies, submitting proposed standards and guidelines to OMB for promulgation, conducting security research, developing security performance indicators, evaluating private sector information, security policies and also reporting annually to OMB among others.

Additionally germane to NIST's key security responsibilities, H.R. 3844 would establish an Office for Information Security Programs at NIST which the director would be responsible for administering. NIST information security responsibilities, under FISMA, authorize a $20 million level funding for NIST's security program, rename the computer security system and Privacy Advisory Board as the Information Security Board with new responsibilities, as well as eliminating the existing process under limited and specified circumstances for agencies to waive the use of mandatory and binding security standards.

The Department believes that overall, the drafters of the bill are to be commended for taking a sound and practical approach to information security, one that will serve the Nation well in the years ahead. The bill appropriately maintains existing separation of responsibilities for security and sensitive systems, which is a major concern for the IT industry.

Current NIST activities are well aligned with the majority of the bill's provisions and additional activities, specific assignments and also the envisioned growth of NIST in the cyber security program will further strengthen the security of all Federal security agency systems. Moreover, the bill will promote the consistencies in the protection accorded to similar systems and information across the entire Government.

Let me respectfully offer, however, the Department's specific concerns on the bill for the committee's consideration. I am mindful of the time constraints I have so let me just run over them in general. I would be happy to respond to them at a later point in the questions.

One is proposed transfer authority to issue standards and guidelines from the Secretary of Commerce to the Director of OMB. We believe that should be reconsidered because the Secretary represents industry and that is an inherent function of the Secretary.

In the bill there are also a number of references to the standards development role of OMB. We believe that OMB develops and issues broad security policy and guidance and this should be clarified vis-a-vis what NIST does in collaboration with OMB.

The third concern has to do with the agency's current limited ability to waive mandatory and binding standards.

Finally, the bill would also require that NIST provide OMB with an annual report regarding major deficiencies in information security at Federal agencies and since NIST's responsibilities do not extend to providing day-to-day operational security for Federal systems and Federal agencies, any such report we believe would be woefully incomplete.

I want to close by emphasizing that our national commitment to improving cyber security must be increased in Federal agencies

and elsewhere. As Congressman Davis' bill reemphasizes, there is much more to be done as we address cyber security in the Federal Government. The NIST cyber security program has a proven track record of success and stands ready to work with you, the committee and other Federal agencies in the enhanced role envisioned in FISMA.

Thank you very much.

[The prepared statement of Mr. Wu follows:]

Statement of
Benjamin H. Wu
Deputy Under Secretary for Technology

Technology Administration
U.S. Department of Commerce

Before the

Committee on Government Reform

Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations

Subcommittee on Technology and Procurement Policy

House of Representatives
United States Congress

"Views on H.R. 3844, the Federal Information Security Management Act of 2002"

May 2, 2002

Good morning Chairman Horn and Members of the Subcommittee. On behalf of the Department of Commerce's Technology Administration and its National Institute of Standards and Technology (NIST), thank you for the invitation to speak to you today. I am Ben Wu, Deputy Under Secretary for Technology at the Department of Commerce. I am pleased to be here with you today to share with you the Department's views on H.R. 3844, the Federal Information Security Management Act of 2002. I note that the Administration is still developing a position on H.R. 3844.

Let me first commend you, Mr. Chairman, and the entire Subcommittee for continuing your focus on the critical issue of cybersecurity in Federal departments and agencies. Today's hearing will again remind Federal agencies that cybersecurity must be addressed in a comprehensive manner on a continuing basis. Like other elements of homeland defense, we are unlikely to ever be "finished" with cybersecurity. It demands the continuing attention of the Congress, the Executive Branch, industry, academia, and the public.

The NIST security program supports the nation's homeland defense effort as well as E-Government by enabling improvements in service to our citizens through secure electronic programs. As I will discuss in greater detail shortly, in the area of cybersecurity, NIST has specific statutory responsibilities for Federal agencies under the Computer Security Act of 1987 and follow-on legislation, including the Government Information Security Reform Act (GISRA). NIST is responsible for developing standards and guidelines to assist Federal agencies in the protection of sensitive unclassified systems. This is in addition to our broad mission of strengthening the U.S. economy – including improving the competitiveness of America's information technology (IT) industry. In support of this mission, we conduct standards and technology work to help industry produce more secure, yet cost-effective, products, which we believe will be more competitive in the marketplace. Having more secure products available in the marketplace will, of course, also benefit Federal agencies, because they principally use commercial products to construct and secure their systems.

NIST's Computer Security Division in our Information Technology Laboratory (ITL) is the focal point of our cybersecurity program. We focus on a few key areas: cryptographic standards and applications; security research; security management; and security testing. Our testing program includes both the National Information Assurance Partnership (a joint NIST and the National Security Agency program) and the Cryptographic Module Validation Program (a joint NIST and Government of Canada program).

In his testimony to you on March 6, 2002, Dr. Arden Bement, the Director of NIST, provided a broad-ranging review of NIST's activities undertaken to fulfill our important cybersecurity responsibilities. For the sake of brevity today, I would simply encourage

you to see his testimony for details. (Available on line at http://www.nist.gov/testimony/2002/abgisra.html)

NIST's Current Statutory Responsibilities

The Computer Security Act of 1987 was established to improve security and privacy of sensitive[1] information in Federal computer systems. In the realm of protecting sensitive unclassified information and systems, the Act assigned NIST responsibility to:

- Develop uniform security standards and guidelines for the protection of Federal computer systems within the Federal government;
- Develop technical, management, physical and administrative standards and guidelines for cost-effective protection of sensitive information and Federal computer systems;
- Develop guidelines for use by operators of Federal computer systems in training their employees in security awareness and good security practices;
- Develop validation procedures to evaluate the effectiveness of the security standards and guidelines developed;
- Assist the private sector, upon request, in using and applying NIST standards and guidelines;
- Provide technical assistance to operators of Federal computer systems in implementing these standards and guidelines; and
- Coordinate closely with other agencies such as the Departments of Energy and Defense, the Office of Management and Budget, and others as appropriate, to assure to the maximum extent feasible that standards and guidelines developed are consistent and compatible across the entire Federal sector (classified and sensitive unclassified).

These NIST responsibilities for the security of Federal sensitive systems were re-emphasized under the Government Information Security Reform Act (GISRA) in 2000. Under GISRA, NIST is tasked to:

---

[1] The Computer Security Act provides a broad definition of the term "sensitive" information: "any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy." Note that this definition implies that sensitive information does not necessarily require confidentiality protection, as does national security (i.e., classified) information.

- Develop, issue, review and update standards and guidance for security of Federal information systems;

- Develop, issue, review and update guidelines for training in computer security awareness and accepted computer security practices;

- Provide agencies with guidance for security planning to assist in development of applications and system security plans;

- Provide guidance and assistance to agencies on cost-effective controls for interconnecting systems; and

- Evaluate information technologies to assess security vulnerabilities in Federal systems.

Proposed NIST Responsibilities under the Federal Information Security Management Act

Under FISMA, NIST would have the following key responsibilities:

- Develop IT standards and guidelines, including minimum requirements, for information systems;

- Develop security standards and guidelines, including minimum requirements, for the security of non-national security systems within the Federal government;

- Specifically develop guidelines for: 1) categorizing all Federal information and information systems according to a range of risk levels; 2) the types of information systems in each category; 3) minimum security requirements for information and information systems in each category; 4) detecting and handling Federal information security incidents; and 5) identification of national security systems within the Federal Government;

- Consult with other agencies to assure: 1) use of appropriate information security policies and procedures; 2) duplication of effort is avoided; and 3) that standards and guidelines are complementary with those employed to protect national security information and systems;

- Provide assistance to agencies on 1) complying with NIST-developed standards and guidelines; 2) detecting and handling security incidents; and 3) security policies, procedures, and practices;

- Submit proposed standards and guidelines, accompanied by recommendation of the extent to which they should be made compulsory and binding, to the Director of the Office of Management and Budget (OMB) for promulgation;

- Conduct security research;
- Develop security performance indicators;
- Evaluate private sector information security policies and practices for potential use in the government;
- Solicit recommendations of the Information Security Advisory Board on proposed standards and guidelines and also submit those to the Director of OMB; and
- Report annually to OMB on: 1) compliance with Clinger-Cohen requirements; 2) major deficiencies in Federal security; and 3) recommendations for improvement.

Additionally, germane to NIST's key security responsibilities, FISMA would:

- Establish an Office for Information Security Programs at NIST, the director of which would be responsible for administering NIST's information security responsibilities under FISMA;
- Authorize a $20 million level funding for NIST's security program;[2]
- Rename the "Computer System Security and Privacy Advisory Board" as the "Information Security Board," add the Director of OMB (and delete the Secretary of Commerce) as a customer for the Board's advice, and authorize funds for its operation; and
- Eliminate the existing process, under limited and specified circumstances, for agencies to waive the use of mandatory and binding security standards.[3]

Comments on FISMA

Overall, the drafters of the bill are to be commended for taking a sound and practical approach to information security, and one that will serve the nation well in the years ahead. The bill appropriately maintains the existing separation of responsibilities for Federal national security and sensitive systems. Current NIST activities are well aligned with the majority of the bill's provisions, and the additional activities, specific assignments, and envisioned growth of the NIST cybersecurity program will further

[2] Currently, approximately $10 million of direct Congressional appropriations funds the NIST security technical staff of about 45 to support our Computer Security Act responsibilities.

[3] Under the Computer Security Act and a November 14, 1988 delegation of authority from the Secretary of Commerce, agencies may waive the use of mandatory standards when compliance would adversely affect the accomplishment of an agency's mission or cause a major adverse financial impact that is not offset by governmentwide savings. Agencies must notify the Congress and publish a notice in the Federal Register of such decisions.

strengthen the security of Federal agency systems. Moreover, the bill will promote consistency in the protection accorded to similar systems and information across the entire government. Generally speaking, increasing the funding of the NIST program is consistent with the President's budget proposal, although the amounts proposed in the bill exceed those in the Administration's budget. I would respectfully offer the following specific comments on the bill for the Committee's consideration.

The proposed transfer of authority to issue standards and guidelines from the Secretary of Commerce to the Director of OMB should be reconsidered. The Director of OMB issues broad information security policy and guidance to agencies complemented by the detailed security standards and guidelines developed by NIST. The proposed process presents the opportunity for delay as additional senior managerial approvals would be required. Instead, as we fight the war on terrorism, we should be thinking about how to streamline the development and issuance of security standards, while still maintaining the important process of public review and comment. Because NIST activities are more directly and immediately accountable to the Secretary of Commerce, it is appropriate that his authority be retained in this regard. The Secretary's strong and continuing engagement with industry also brings an important perspective to the standards development process.

In the bill there are also a number of references to the "standards development" role of OMB. Since OMB develops and issues broad security policy and guidance, this should be clarified vis-à-vis NIST's role to develop standards and guidelines within the Federal Government.

The third comment has to do with agencies' current limited ability to waive "mandatory and binding" standards. As you know, the Federal government is an exceedingly large and diverse environment -- with operations from Moscow to Honolulu to Washington -- with an even wider variety of sensitive and not-so-sensitive information and systems. The present approach, with its very public process of Congressional and public notice process (in the Federal Register) strongly discourages the waiving of mandatory standards. After all, there have only been a handful of security waivers since the passage of the Computer Security Act. In the field of security, like all others, we must spend Federal resources wisely in accordance with sound risk management. Eliminating this option may lead to wasteful or misapplied spending because, in some situations, there may be alternate security measures that effectively allow the agency to meet the same overall security *objective*, although not the letter of the standardized security method. For these reasons, we believe it makes sense to maintain the current approach.

Lastly, the bill would require that NIST provide OMB with an annual report regarding major deficiencies in information security at Federal agencies. Since NIST's responsibilities do not extent to providing day-to-day operational security for Federal agencies, any such report would be woefully incomplete. However, OMB will still obtain the necessary information under FISMA since its provisions, like those of GISRA, require agencies to provide OMB with a report of their independent security evaluations. OMB thus obtains a very direct and unfiltered view of the security posture of the agencies. I would note that this information would also be useful to NIST to help

identify potential needs of the agencies for additional security standards and guidelines (or modifications to those already existing). Therefore we request that this NIST reporting requirement be deleted as unnecessary and duplicative. Of course, we always stand ready to provide OMB with any additional information they may require.

We would welcome the opportunity to continue its discussions with the drafters to further refine the bill to address these and a few other very minor concerns that we have.

Conclusion

Let me close by emphasizing that our national commitment to improve cybersecurity must be increased -- in Federal agencies and elsewhere. As Representative Davis' bill again re-emphasizes, there is much more to be done to address cybersecurity in the Federal government. The NIST cybersecurity program has a proven track record of success and stands ready to play the enhanced role envisioned in FISMA.

Thank you, Mr. Chairman for the opportunity to present our views today on FISMA. I will be pleased to answer any questions that you and the other members of the Committee may have.

Mr. HORN. We appreciate your testimony and we will get into that in the question period shortly.

Our next witness is Ronald E. Miller, Chief Information Officer and Assistant Director, Information Technology Services Director, Federal Emergency Management Agency, FEMA. That is a very fine agency. Over the last 10 years, they have really put their act together and with all the problems that have come forth with tornadoes, floods, you name it, they have done great work with all of us in the Congress.

Mr. Miller, you have a very fine record in the military. We are glad to see you here.

Mr. MILLER. Thank you, Chairman Horn, Chairman Davis and members of the committee.

I would like to take the opportunity to thank you for addressing this very important issue and while I cannot present the administration's view, I would like to share both FEMA's position on information security and my perspective as the security liaison for the CIO Council.

Very briefly I want to spend a few moments talking about FEMA's approach to IT security. It is fairly straightforward. As a Federal agency, we are required to deliver mandated products and services and we must do so in full compliance with laws of the land. That includes the security requirements put forth in public laws, executive branch directives, Federal standards and agency-specific policies. We view those requirements as being the minimum set of security standards that we must comply with in the development of our systems, so that in that regard we want to include a certain set of steps to take for every system we implement. Those steps include formally certified system security plan, formal accreditation and approval to operate by the appropriate management official, tested contingency plans, implemented incident handling capabilities, security education awareness program and a capital plan for funding security across the systems life cycle.

Our approach is to use a well disciplined capital planning and investment process and ensure security costs are incorporated into the system development life cycle. Our capital planning process is strongly linked to the agency's performance plan and goals. Using this approach, we have created a framework whereby IT solutions are implemented to support prioritized agency mission requirements and security is made a part of the IT solution itself. In this manner, we are also able to determine that the resources we apply to our IT security activities are directly aligned with the agency's performance goals.

With regard to GISRA, there are noticeable improvements in the area of IT security because of the enactment of that legislation because it helped put management focus on this important problem. We still have need for additional progress and believe that FISMA is sound and will help.

The CIO community overall views GISRA as a very positive step forward because it codified many of the requirements put forth in OMB Circular 30. The codification of those requirements signaled a heightened awareness on the part of the legislative branch concerning the importance of implementing adequate IT security. It also helped to clarify the role of the Chief Information Officer as

being responsible for implementing an adequate IT security program across the agencies. It required that a senior official be designated to head IT security and that official would report directly to the CIO.

We find the annual report requirement to be particularly useful because it allows us to not only gain a full perspective on the state of our security programs, but it also ensures that the state of IT security is well documented and understood by senior agency managers. In general, we see FISMA as similar to GISRA in most regards and we are confident in our abilities to implement if enacted.

There are areas where we believe the bill needs improvement and we would like to see it address the following. First, we would like to see a stronger link between IT security requirements and the capital planning process, stronger emphasis on resources for IT security training, the retention of IT security professionals, support for day to day security efforts and individual accountability for security.

We need to ensure that capital planning investments include consideration for security which is a powerful incentive for program officials. We believe we need a work force that is well trained and prepared to address the complex issues found in IT security and an emphasis should be placed on providing resources that provide training to employees responsible for implementing these standards.

We also believe we need to look to retaining the work force once we have recruited and trained folks that are skilled in IT security. We support the administration's Managerial Flexibility Act which would allow Federal agencies the flexibility to provide hiring and retention incentives to potential employees, including IT security professionals.

There needs to be overarching support for the day to day security efforts across the Federal Government such as CERT, the FedCIRC, incident support, patch distribution service is just beginning at GSA, training and guidelines and soon. We need to hold Federal Government officials individually responsible in their performance plans for the implementation of security within their programs. OMB has certainly taken a step in the right direction with the balanced score card.

The world has changed in many ways since September 11th and I believe that with the concept of electronic government, the security requirements are more prevalent now than ever before. I am looking forward to working with the committee and each one of you in helping the Federal Government address needed improvements in Federal IT security.

Thank you for this opportunity. I look forward to questions at the end of the testimony.

[The prepared statement of Mr. Miller follows:]

Statement of
Ronald E. Miller
Chief Information Officer
Federal Emergency Management Agency
Committee on Government Reform
Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations
Subcommittee for Technology and Procurement Policy
U.S. House of Representatives

May 2, 2002

Good morning, Mr. Chairman and Members of the Committee. I am pleased to be here today to talk about information technology security. Although I am not in a position to express the Administration's views on H.R. 3844, the 'Federal Information Security Reform Act of 2002,' or 'FISMA', I thought it would be useful to share FEMA's experience with the Subcommittee. I understand that FISMA would reauthorize and amend the Government Information Security Reform Act ("GISRA") and would like to share both my agency's experiences with GISRA and my perspective as the CIO Council's Security Liaison.

My testimony today will include topics in the following areas:

- FEMA's Approach to Information Technology ("IT") Security
    - Philosophy

- Minimum Standards
- Performance Goals
- Capital Planning and Investment Process

- GISRA Experience
  - General Comments
  - What We Like Best

- FISMA Comments
  - General Comments
  - Potential Areas for Improvement

- Moving Forward
  - Strategic Directions

FEMA's Approach to Information Technology ("IT") Security

I would like to spend just a few moments describing FEMA's approach to IT security. Our approach to IT security strongly shapes our opinions concerning GISRA and the pending legislation known as FISMA.

FEMA's IT security philosophy is fairly straightforward. As a federal agency, we must deliver mandated services and products, and we must do so in full compliance with the laws of the land. What this means for us is that as we implement IT solutions to support our business processes, we must ensure that the IT solutions incorporate the security requirements put forth in public laws, Executive Branch directives, federal standards, and agency-specific policies.

We view the mentioned security requirements as providing the minimum security standards for our systems. A critical component of our process is ensuring that

all of our information systems meet a minimum set of standards. These standards are consistent with public laws and include:

- A formally certified system security plan
- Formal accreditation and approval to operate by the appropriate management official
- Tested contingency plans
- Implemented incident handling capabilities
- Security education awareness program
- Capital plan for funding security across the system's lifecycle

Our approach is to use a well-disciplined capital planning and investment process that ensures security costs are incorporated into the system development lifecycle. Our capital planning process is strongly linked to the agency's performance plan and goals. Using this approach, we have created a framework whereby IT solutions are implemented to support prioritized agency mission requirements and security is made a part of the IT solution itself. In this manner we are also able to demonstrate that the resources we apply to our IT security activities are directly in line with the agency's performance goals.

GISRA Experience

Overall, there are noticeable improvements being made across the Federal government in the area of IT security. GISRA has helped put management focus on this important problem. We still have need for additional progress, however, and FISMA is sound and will help.

The CIO community overall views GISRA as a very positive step forward for improving IT security in the federal government. GISRA codified many of the requirements put forth in OMB A-130. The codification of the A-130 requirements signaled a heightened awareness on the part of legislative branch

concerning the importance of implementing adequate IT security. The language in GISRA helped to clarify the role of the Chief Information Officer as being responsible for implementing an adequate IT security program across their agency. Also, GISRA required that each agency designate a senior official to head their IT security program and report to the Chief Information Officer.

An aspect of GISRA that we have found to be particularly useful is the annual report. The annual report is developed from program reviews conducted by the Chief Information Officer and combined with an independent assessment prepared by the agency's Inspector General. The development of the annual report is a significant undertaking and provides a significant benefit in terms of ensuring that the state of IT security is well documented and understood by senior agency managers.

FISMA Comments

In general, FEMA sees FISMA as similar to GISRA in most regards. Given the many similarities between FISMA and the existing GISRA we are confident in our abilities to implement FISMA, if enacted.

There are a number of areas in which, from the information security technologist's point of view, the bill needs improvement. For example, the bill should address the following:

- Stronger link between IT security requirements and the capital planning process
- Stronger emphasis and resources for IT security training
- Retention of IT security professionals
- Support for day-to-day security efforts
- Individual accountability for security

OMB has made it clear that IT capital investments must include consideration for implementing adequate IT security. Implementing adequate security requires having adequate resources. OMB's tying the approval of IT spending to a demonstrable security plan would provide a powerful incentive to program officials.

We do believe that in order to implement adequate security, the federal government requires a workforce that is well-trained and prepared to address the complex issues found in IT security. A strong emphasis should be placed on providing resources that provide training to employees responsible for implementing minimum federal standards. It would be very useful if the federal government provided IT security training in perhaps the same way that it offers standardized training in technology subjects, management skills, leadership development, and other professional disciplines.

Developing a well-trained federal workforce is important, but equally important will be our ability to retain this workforce. We support the Administration's Managerial Flexibility Act , which would allow federal agencies the flexibility to provide hiring and retention incentives to potential employees, including IT security professionals. This is particularly important when we consider that a significant portion of the current federal IT workforce will be eligible for retirement over the next 10 years.

There needs to be overarching support for the day-to-day security efforts across the Federal government. Examples include Carnegie Mellon CERT, FedCIRC (incident support), patch distribution services (just beginning at GSA), training, and guidelines (e.g., risk management). .

Finally, there is a strong need to hold federal government officials individually responsible in their performance plans for the implementation of security within their programs.. It has been demonstrated in numerous ways that employees

who have a personal stake in the success of a particular program will generally deliver a higher level of performance. A corresponding side to this is rewarding those employees that do deliver high levels of performance.

Moving Forward

In the future, there will be a need to coordinate with the Office of Homeland Security to leverage the federal government and link with other governmental and industry representatives to provide an effective cyber security capability.

The world has changed in many ways since September 11 last year. We are in a time of major changes in our approach to delivering emergency management services. It is very clear from the priorities expressed by OMB that electronic government is, and will continue to be, a major strategic direction for the federal government. The concept of electronic government will greatly change the manner in which we do business. To realize the full potential of electronic government, we must be able to implement electronic information sharing horizontally between government agencies, vertically from the federal government to the states, and very importantly, to the American public. An enabling factor will be our ability to implement and enjoy the benefits of electronic government, and do so in a manner whereby the risk does not outweigh those benefits.

Close

I am looking forward to working with this committee and each one of you in helping the federal government address needed improvements in federal IT security. Thank you for the opportunity to be here today. I will be happy to answer any questions you may have.

Mr. HORN. Thank you.

Next is David C. Williams, Inspector General of quite a few agencies. He started out, I suspect, being a Special Agent in both the U.S. Secret Service but also in U.S. military intelligence. He is a recipient of a U.S. Bronze Star and the Vietnamese Medal of Honor. We are delighted to have you here.

I had one question on the Inspector General role with the Tax Administration. Was that to deal with the 100,000 people that are in IRS or the clients they deal with?

Mr. WILLIAMS. I believe we have a very strong commitment toward their clients, the taxpayers and certainly as represented through the House and Senate committees. Our coverage involves the activities of the Tax Administration, which is both the IRS and some policy units inside main Treasury.

Mr. HORN. Great. Go ahead with your summary.

Mr. WILLIAMS. I appreciate the opportunity to appear today to provide an Inspector General's perspective.

Government agencies continue to struggle with the appropriate balance between IT security and computing capacity, too often with an overwhelming bias toward speed and ease of operations. The Government Information Security Reform Act has served as an essential beacon urging agencies toward a more balanced course. During fiscal year 2001, the GISRA assessments identified substantial vulnerabilities across government that could threaten the security of information systems. These included formal security training and awareness programs for all employees were frequently ineffective or nonexistent.

In the IRS for instance, 70 of 100 employees were willing to compromise their passwords during pretext telephone calls by IG auditors. No matter how strong other controls may be, employees can often be the most vulnerable component of an agency's IT security program.

Specific performance measures were often absent such as the effectiveness of efforts to reduce the impact of computer viruses. Oversight of contractors was not sufficient and many had not received the necessary background clearances. An unacceptable number of systems and applications critical to the agency missions were not security certified or accredited. System intrusion incidents were not consistently reported and shared throughout the Government to assist agencies to proactively identify and combat hacking. Security controls often seem to be an after thought in IT budget investment decisions and senior managers often assumed little responsibility for IT security within their programs, deferring entirely to small security offices.

To increase the likelihood of success, agencies need to be held accountable for their security programs. Some agencies appear to view the GISRA annual reporting process as a pro forma exercise. To assure GISRA effectiveness funding requests for IT initiatives should be contingent on the integration of adequate security controls. To assist agencies in adhering to GISRA and H.R. 3844 provisions, we offer the following suggestions to improve the consistency in conducting and reporting information security assessments and investigations.

Certain terminology should be clarified to avoid confusion in reporting. Terms such as programs, systems, networks, mission critical and mission essential are subject to varying interpretations. Agency officials should be required to use the NIST IT security assessment framework. Agency and IG reporting requirements should be integrated to reduce duplication of effort. The OMB should provide implementation and guidance at the beginning of each reporting year. Annual submissions should contain a conclusions section on agency compliance with the law and its overall information security posture.

The IG should be required to evaluate whether agencies have a process that incorporates information security into their enterprise architectures. Reporting intrusion incidents to Fed CIRC should not be limited to national security incidents but should also include threats to critical infrastructure as was the case during the Y2K initiative.

Importantly, agencies should identify the IG or another law enforcement agency that will investigate intrusions and refer them for prosecution.

In conclusion, while it is still early in the GISRA implementation process, we are optimistic that if enforced, GISRA and its successor legislation will ultimately succeed in strengthening information security throughout the government.

I would be happy to answer questions at the appropriate time.

[The prepared statement of Mr. Williams follows:]

JOINT HEARING BEFORE THE

SUBCOMMITTEE ON GOVERNMENT EFFICIENCY, FINANCIAL MANAGEMENT AND INTERGOVERNMENTAL RELATIONS

AND

SUBCOMMITTEE FOR TECHNOLOGY AND PROCUREMENT POLICY

COMMITTEE ON GOVERNMENT REFORM
U.S. HOUSE OF REPRESENTATIVES

MAY 2, 2002

H.R. 3844 "FEDERAL INFORMATION AND SECURITY REFORM ACT OF 2002"

STATEMENT FOR THE RECORD

DAVID C. WILLIAMS
INSPECTOR GENERAL
TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Mr. Chairmen, and members of the subcommittees, I appreciate the opportunity to appear today to provide an Inspector General's (IG) perspective. Government agencies continue to struggle with the appropriate balance between IT security and computing capacity, too often with an overwhelming bias toward speed and ease of operations. The Government Information Security Reform Act (GISRA) has served as an essential beacon urging agencies toward a more balanced course. During Fiscal Year 2001, the GISRA assessments identified substantial vulnerabilities across government that could threaten the security of information systems. These included:

- Formal security training and awareness programs for all employees were frequently ineffective or non-existent. In the Internal Revenue Service, for example, 70 of 100 employees were willing to compromise their passwords, during pretext telephone calls by IG auditors. No matter how strong other controls may be, employees can often be the most vulnerable component of an agency's IT security program.
- Specific performance measures were often absent, such as the effectiveness of efforts to reduce the impact of computer viruses.
- Oversight of contractors was not sufficient and many had not received the necessary background clearances.
- An unacceptable number of systems and applications critical to the agency missions were not security certified and accredited.

- System intrusion incidents were not consistently reported and shared throughout the government to assist agencies to proactively identify and combat hacking.
- Security controls often seemed to be an afterthought in IT budget and investment decisions, and
- Senior managers often assumed little responsibility for IT security within their programs, deferring entirely to small security offices.

To increase the likelihood of success, agencies need to be held accountable for their security programs. Some agencies have appeared to view the GISRA annual reporting process as a pro forma exercise. To assure GISRA effectiveness, funding requests for IT initiatives should be contingent on the integration of adequate security controls.

- To assist agencies in adhering to GISRA and H.R. 3844 provisions, we offer the following suggestions to improve consistency in conducting and reporting information security assessments and investigations.
- Certain terminology should be clarified to avoid confusion in reporting. Terms such as "programs", "systems", "networks", "mission-critical" and "mission essential" are subject to varying interpretations.
- Agency officials should be required to use the NIST IT security assessment framework.

- Agency and IG reporting requirements should be integrated to reduce duplication of effort.
- The OMB should provide implementation guidance at the beginning of each reporting year.
- Annual submissions should contain a conclusion section on agency compliance with the law and its overall information security posture.
- The IGs should be required to evaluate whether agencies have a process that incorporates information security into their Enterprise Architectures.
- Reporting intrusion incidents to FedCIRC should not be limited to national security incidents, but should also include threats to critical infrastructure, as was the case during the Y2K initiative, and
- Importantly, agencies should identify the IG or another law enforcement organization that will investigate intrusions and refer them for prosecution.

In conclusion, while it is still early in the GISRA implementation process, we are optimistic that, if enforced, the GISRA and its successor legislation will ultimately succeed in strengthening information security throughout the government.

I would be happy to answer any questions.

Mr. HORN. Thank you.

Our last presenter before the questioning is James Dempsey, Deputy Director, Center for Democracy and Technology. You have a very rich background and I note here that with a Professor David Cole. What university was he with?

Mr. DEMPSEY. Georgetown University.

Mr. HORN. You did this book on "Terrorism and the Constitution, Sacrificing Civil Liberties in the Name of National Security." The second edition is out, so you are a well designed author with a second edition in 2002 as well as journal articles, and a background of Yale and Harvard Law School.

When I was at Harvard, we used to say there was a great operation at Yale but they would come to Harvard for an education. So you covered both, you and the Bush family have covered all of them.

You are a member of the District of Columbia Bar. Tell us a bit about the Center for Democracy and Technology.

Mr. DEMPSEY. Good morning, Mr. Chairman, Chairman Davis and Congresswoman. Thank you very much for inviting us to testify this morning on the important issue of the security of Federal Government computer systems.

The Center for Democracy and Technology is a non-profit, public interest organization. Our goals include enhancing privacy protections for individuals and preserving and promoting the democratic potential of the Internet. We work closely with industry and with policymakers to develop balanced policy solutions to the information technology issues that face both the Government and the private sector. We focus much of our attention on the Internet because we believe that, more than any other medium, it has characteristics that are uniquely supportive of democratic values. The Internet has the power to enhance the delivery of Government services, to provide cost efficiencies for government, businesses and individuals, and to facilitate interaction between the Government and its citizens.

Hanging over that and potentially threatening that potential is the vulnerability of computer networks, which also affects fundamental government operations and the private sector, and the economy as well.

Unlike the gentlemen who testified before me who are very much in the trenches dealing with this issue, I am going to take, if I could, a somewhat broader perspective, looking at the issue of government information system security in a somewhat broader context.

I want to congratulate you, Chairman Horn, and Chairman Davis, for your leadership in addressing this issue in a comprehensive and serious way. I commend you for bringing forward H.R. 3844 to build on the important progress of GISRA.

My basic message today is that, in developing and implementing policy solutions for the security deficiencies that exist in government computer systems, it is imperative to recognize and preserve the open, innovative, and interactive nature of the medium and to use that to promote the government objectives that all of these agencies are so nobly trying to advance.

In creating a standard, setting policy for government computer systems, we urge you to draw upon the expertise of the private sector. Chairman Davis referred to the importance of having flexibility and to recognize the speed with which this technology is developing, and to buildupon developments within the private sector where systems designers and managers are grappling with these same issues of balancing security, efficiency, privacy and openness.

On the point of privacy particularly,k we believe that it needs to be a part of the equation of computer security. If you look at any of the legislation and the fair information principles going back to the 1970's, privacy and security always went hand in hand.

I have four basic suggestions or comments on the legislation today. One is to focus on government computer systems not information per se. The question of management of government information generally, its security, disclosure, privacy, is a very complicated subject. With lots of legislation, while clearly what we are talking about today is the unique challenges, threats and difficulties posed by networked computer systems. Yet if you look at the legislation, it refers to information and information systems. I think all of the focus here at the table is on information systems which pose these unique, documented vulnerabilities and the need for some top down leadership within the Government to get the Government's security house in order. That should be the focus and I think unintentionally perhaps the legislation is a little misleading in that regard.

Second, is to recognize and promote a balanced approach. Security needs to be dealt with in tandem with privacy, openness and efficiency, which are the four interests I think the goal is to balance. In looking at the legislation as it is drafted, I don't think that balancing point comes through clearly enough.

Third, it is necessary, particularly at this time, to preserve and enhance within the executive branch a privacy advisory function. The bill would amend the charter of the Computer Systems Security and Privacy Advisory Board as I read it to remove privacy from the jurisdiction of that body and at this time, I think it is very important to have within and available to the Federal Government an advisory function that looks at the privacy implications of computer system design and other information issues facing the Government.

Fourth, just to repeat the point about working with, and consulting with a broad range of interests within the private sector where there is obviously a tremendous amount of energy and attention being given to these computer security issues. These are the people designing the systems. Some of the same problems and vulnerabilities that the Government is grappling with are recognized in the private sector as well.

We would look forward to working with you. I look forward to answering your questions. Thank you again for inviting COT to testify today.

[The prepared statement of Mr. Dempsey follows:]

May 16, 2002

The Honorable Steve Horn
Chairman
Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations
House Committee on Government Reform
B-373 Rayburn HOB
Washington DC 20515

The Honorable Thomas M. Davis III
Chairman
Subcommittee on Technology and and Procurement Policy
B-349 Rayburn HOB
House Committee on Government Reform
Washington, DC 20515

Dear Chairman Horn and Chairman Davis:

Thank you again for the opportunity to testify at the May 2, 2002 joint hearing of your subcommittees regarding H.R. 3844, the "Federal Information Security Reform Act of 2002." During that hearing, Chairman Horn asked me to expand upon a point I had made in my written testimony, namely, that there is an increasingly widely accepted set of practices developed by the private sector that agencies ought to be adopting. I am pleased to submit the following information, compiled with the assistance of Alan Paller, Director of Research at the SANS Institute.

The sets of practices that are most important for protecting federal systems are detailed configuration guidelines that protect systems from probes and attacks launched by automated programs that scour the network looking for vulnerable systems. Such configuration practices can be especially effective when accompanied by testing tools that verify that the guidelines have been followed, that provide scores for each system and that provide specific guidance for correcting any problems uncovered by the testing tools.

Four organizations – two federal (NSA and NIST) and two representing large segments of the private sector in the US and internationally (the Center for Internet Security and the SANS Institute) – have developed guides of "accepted practices" for configuring information systems safely. Their guides are listed below along with URLs where they can be acquired.

Recently, under NIST's leadership, the four organizations have made substantial headway in eliminating differences between their guidance. On April 18 technical experts responsible for the Windows 2000 guides from all four organizations met at NIST and hammered out a consensus on the minimum security settings for any Windows 2000

systems connected to the Internet. GSA and several other federal agencies have joined the original four organizations so that federal system administrators can receive consistent guidance.

The consensus that has been reached on Windows 2000 provides four major benefits for federal agencies and their IT, security, and IG staffs:

1. They can use procurement to improve security by ordering new systems configured safely "out of the box."
2. Auditors and systems managers can use the same tools for testing systems -- avoiding unnecessary conflicts based on differences in experience between the two groups. The Center for Internet Security provides free testing tools that measure systems against the benchmarks.
3. System administrators can automate the process of configuring systems and share the automated tools among agencies -- radically reducing the number of systems that are configured unsafely because of lack of system administrator experience.
4. Application developers and vendors can test their systems on safely configured systems -- leading to a future where configuration changes have much less chance of disabling applications, and reducing the pain associated with securing systems.

The work done on building a consensus for Windows 2000 will soon be replicated for Cisco IOS systems and Sun Solaris systems. Other systems will follow.

The four sets of guides (in chronological order of when they were released) are:

1. The SANS Institute Step-by-Step Guides - www.sansstore.org

-- Securing Windows 2000: Step-by-Step
-- Windows NT Security: Step-by-Step
-- Solaris Security: Step-by-Step
-- Securing Linux: Step-by-Step
-- Computer Security Incident Handling Step-by-Step
-- Disaster Recovery and Business Continuity: Step-by-Step

2. The National Security Agency Configuration Guides -- available at www.nsa.gov

Windows 2000 Guides
Windows NT Guides
Guide to Securing Microsoft Windows NT Networks
Cisco Router Guide
Router Security Configuration Guide
E-mail and Executable Content Guides

3. The Center for Internet Security Guides and automated testing tools -- available at www.cisecurity.org

- Linux Security Benchmarks and testing tools
- HP-UX Benchmarks and testing tools
- Cisco IOS Router benchmarks and testing tools
- Windows 2000 benchmarks and testing tools
- Solaris benchmarks and testing tools

4. The National Institutes of Standards and Technology -- available at http://csrc.nist.gov/publications/drafts.html

Special Publication 800-43, System Administration Guidance for Windows 2000 Professional

In my oral testimony, I mentioned the Common Criteria. The Common Criteria are a set of detailed technical guidelines for the design of computer system components, plus a network of testing laboratories around the world that can test products. The Common Criteria are very useful, but because their focus is on design, a system that meets the Common Criteria can still be insecure. A simple example is a firewall that meets the CC but is configured to "allow all traffic." Therefore, the Common Criteria need to be used in conjunction with the configuration guides referenced above. In essence, the configuration guides offer a second level of common criteria that might be called common configuration criteria.

Finally, as suggested above, several entities are developing testing tools that can verify that the configuration practices have been followed, that provide scores for each system and that provide specific guidance for correcting any problems uncovered by the testing tools. The Center for Internet Security (CIS) is updating its free testing and scoring tools. Symantec and Bindview are building commercial versions of the testing tools.

In sum, it is widely recognized that most of the damage being done to computer systems is carried out by exploiting known vulnerabilities for which there are known remedies. The challenge facing systems managers is to get the known remedies installed and used. It was the thrust of the final section of my testimony that the foregoing standards can dramatically improve the level of government computer security, if an agency with government-wide clout can do ensure that agencies use them.

Again, please let me know if I can assist you in any way.

Sincerely,

James X. Dempsey
Deputy Director

Mr. HORN. Thank you.

We now yield 10 minutes to the gentleman from Virginia to begin the questioning.

Mr. DAVIS. My intent for the Incident Center was not to create multiple centers or to duplicate existing centers, but to ensure that there be at least one governmentwide center and that it have a strong statutory mandate to provide effective instant response and assistance to all agencies.

The bill makes it very clear that it is up to OMB to ensure that such a center is established. Does anyone have a problem with the Federal Government having a strong central information security incident response?

Mr. WILLIAMS. Not only do I not have a problem, I think it is a very good idea. At this point, we don't have a very mature process for identifying the kinds of incidents to be forwarded, we are still feeling our way through dissemination and with regard to dissemination of the information once we gather and analyze it. There is not necessarily a strong, consistent way of dealing with the incidents once we identify them. We don't want them just to pass, we want to aggressively move against them where the intrusion has been illegal.

We need something like this. This is pointed in the right direction, it is a void and I am for it.

Mr. FORMAN. I think clearly as indicated in my testimony, that is the direction we have been moving within the executive branch in how we have been using FedCIRC and the capabilities they have been building. The corollary to creating the organization is the process and that is what is really lacking. We need to not just think about the annual reporting and risk management process. When you deal at the incident level, you deal basically within 24 hours as a cycle of time. That means we have to have a very streamlined, fast and responsive process to the vulnerabilities and the threats. It is a 3 x 3 matrix of potential risks, vulnerabilities, and responses the agencies have to look at.

This is clearly one of the areas where we definitely agree. Things need to be done and I would go so far as to say, not just in the organization itself, but in the type of streamlining process, reporting response requirements. There should be some guidance.

Mr. WOLF. In my testimony, I stated that we have several centers set up and we interact with them on a routine basis. I think it is important that you emphasize in terms of what gets reported and the processes of how all that gets put together.

Mr. DEMPSEY. Just one comment. I think the prior administration stubbed its toe on this issue to some extent when it talked about the FIDNET intrusion detection monitoring system and put that forward without adequately considering the privacy issues that posed. I think that is a classic example of how privacy should be built into decisionmaking and development processes because I think while there is tremendous merit to a centralized information security incident center, some of the issues of intrusion detection do raise obvious privacy issues that need to be addressed or otherwise the thing is going to run into criticism and potential problems again.

Mr. MILLER. From the perspective of an agency, my hope is that we have a center of excellence to support what we are trying to do in the area of IT security. It may be more of a process issue than an organizational issue, but the bottom line for us is that we need help in getting that kind of support. If we can bring the resources of the Federal Government together in such a way that they can provide us with that center of excellence we can report to, that we can get advice and counsel from in security matters, and that we can get some form of assistance when we have a critical incident, then that is always helpful for us. We don't have enough resources to do it on our own.

Mr. DAVIS. Mr. Wu, will NIST be able to quickly develop the standards and guidelines called for in the bill? Some skeptics have shared concern that NIST is just not up to the task. What do you think?

Mr. WU. NIST is prepared and willing to take on any responsibilities that would be delineated if H.R. 3844 were to be enacted. We would be working in conjunction with OMB but also we would be working with industry.

One concern, however, is the NIST resources. I think you are correct in stating that the current NIST resources may be overtaxed with some of the responsibilities under FISMA, but given the importance of the computer security issue, we would hope that Congress would be kind and look forward to an appropriation that would be a sufficient amount for NIST to take on other responsibilities. But the technical expertise, the energy, and the enthusiasm to take on these responsibilities is there at NIST.

Mr. DAVIS. You understand we are not looking for a specific technical standard that could be quickly outdated and obsolete. We are looking for more specific guidelines and benchmarks to take some of the subjectivity and guesswork out of the process of determining whether an agency has truly done a good job addressing these information security risks.

Mr. WU. NIST is very engaged in the voluntary consensus standards organization process. NIST has worked very closely with industry to make sure that industry concerns are represented and NIST also works with the general public as well and will continue to work with those stakeholders, OMB, and the other Federal agencies.

Mr. DAVIS. Mr. Dacey, one of the significant differences between FISMA and GISRA can be found in the way that FISMA proposes to define national security systems. As you know, GISRA added a third category to the traditional two-part formulation of national security systems and called it debilitating impact systems. GISRA then includes this third category in an exemption in allowing these systems to be excluded from GISRA's information security risk management requirements. Could you expand on this and discuss some of the history and policies involved?

Mr. DACEY. The issues related to, that have to do with that, require you look at the FISMA bill in its entirety. One of the provisions in there is the requirement for establishment of risk levels and minimum standards at those various risk levels. FISMA would include all non-national security systems in the consideration of

that area. So those would be considered at various risk levels and appropriate minimum standards.

One of the concerns that had been expressed during the GISRA implementation was how do you define debilitating impact systems and how will they be treated in the process. They were excluded, as you said, from some of the other areas of GISRA and the provisions of GISRA. This would basically put into place the requirements over those systems that were formerly debilitating impact but also would allow those to be considered in terms of risk assessment and various specified levels of risk.

Mr. DAVIS. I am also interested in the distinctions between national security and non-national security systems. In his prepared statement, Mr. Wolf said there is very little diversity in the underlying technology and therefore, the security vulnerabilities found in national security systems as compared with other Federal systems. It sounds to me like the steps needed to protect national security systems are the same as for non-national security systems. Would you agree with that?

Mr. DACEY. I would agree with the observations that the technologies that are used in both systems have converged and are essentially the same types of technologies. Certainly in the national security systems, they are fairly hardened and strengthened in terms of the level of security placed on them. However, we have a lot of sensitive information, too, in the Federal Government that may require similar levels of protection in the system.

I think in terms of standards, ideally, there would be a coordination between national security and non-national security systems. I think some of the same types of technologies and controls would be relevant to both and in considering the different risk levels for non-national security systems, particularly at the top end with the more secure needs, those could be very consistent with national security requirements.

Mr. WOLF. If I could add one comment, the technologies are very similar. The one thing I would add is that with national security systems, you do have a higher level encryption, stronger encryption than you are dealing with in some of the diplomatic and military activities. So there is a difference there.

Mr. DAVIS. Mr. Dempsey, let me ask you a question. I think we are all concerned with protecting privacy, trying to strike the right balance between national security, critical information security and privacy interests of citizens. Would you agree one of the biggest threats to privacy interest today is the fact that hackers and other unauthorized individuals can break into government information systems and access this personal, sensitive information?

Mr. DEMPSEY. I think that is an important piece of the privacy problem. I think that goes to the complementarity between privacy and security.

Mr. DAVIS. We put walls around a lot of that information so that no one should see it who shouldn't get it and yet a hacker breaks in.

Mr. DEMPSEY. Exactly, and I agree with that. I think some of the interests at stake also in terms of privacy involve the right of individuals under the Privacy Act to access personally identifiable information that is in the hands of the Government. On the one

hand, the goal of privacy is to preserve confidentiality but also under the rubric of privacy we have a broader set of fair information principles, which include the concept of access. That is part of the balance that I was talking about.

I agree with you entirely that one of the goals here is not only to protect government operations but also to protect the huge amount of personal information the government has.

Mr. DAVIS. Mr. Williams, with your extensive experience in law enforcement and IRS, can you share some of your concerns about the seriousness and the threat our Government is facing in the information security area without disclosing too much, the types of problems? That is what we are trying to get at with this.

Mr. WILLIAMS. The threat is serious. We also have the difficulty of this emerging area being one in which we are constantly sort of preparing for the last war, the last attack, rather than being able to look at a completely mature industry and begin to do some dynamic forward looking things. The things that concern us and things we have encountered involve the destruction of information.

We recently caught a contractor who was being discharged who planted a logic bomb inside three of our servers. We were able to halt that but had that gone through, an enormous amount of information would have been lost.

Mr. DAVIS. Does the contractor get debarred for that, are they being appropriately sanctioned?

Mr. WILLIAMS. The person received 3 years in prison.

Mr. DAVIS. How about the contractor?

Mr. WILLIAMS. The contractor was unaware of the incident. We did an extensive lessons learned with the contractor but they appeared to have been as much victimized.

Mr. DAVIS. Can you explain what a logic bomb is?

Mr. WILLIAMS. It was a device triggered when the computer reached a certain capacity which would allow the person time to escape and distance himself from the event. At that point through a system of algorithms, shutdowns and destruction would automatically begin in a remote fashion while the person was separated. I am sure there are some other people who are really good at it but I think that is about how it works.

In addition to the destruction of material, which is more visible, is the theft of material. I am not sure without our shields being up, we really even know how many times we are being raided and sensitive information is being taken. Just at the IRS, and there is the full spectrum of agencies, we have the private financial data of 128 million Americans, there is market sensitive data on there, proprietary data. Those are things of value.

Another type of crime is altering the data in order to gain something of value, in order to have benefits brought to someone that either doesn't exist or doesn't deserve it, or forgiveness of an IRS obligation, manipulating it to wipe out the debt.

Those are some of the different flavors of vulnerability that we have.

Mr. DAVIS. Mr. Chairman, I think my time is up.

Mr. HORN. We are glad to extend the time. It is your bill, we are just trying to get it moving.

Mr. DAVIS. I am satisfied for now.

Mr. HORN. Let us ask the whole panel then, what do you see as the primary challenges to developing and implementing the minimum security standards required by the bill? When we discussed this in the last few days with the staff, I was particularly interested in the Commerce and NIST bit on various standards. I would like Mr. Wu to give me an idea of typical standards we ought to be thinking about.

Mr. WU. There are a number of standards, encryption standards, interoperability standards, all very critical to maintaining an effective computer security infrastructure.

Mr. HORN. What else?

Mr. WU. Our NIST technical and cyber security team have been working with those in industry to identify the remaining standards and other standards that exist and other issues, trying to be forward thinking to try to be able to find out or figure out what vulnerabilities there may be in advance and what we should be looking forward to.

Mr. HORN. And you have a role in that and we need to know what are the levels of the standards, what is the impact in terms of security? Or is it just reacting to some particular case.

Mr. WU. No, it seems clear that when we have major information technology glitches, such as Love Bug and other viruses, that impact not just our Nation but the world, that we need to be much more forward thinking and that we are too reactive. It is important for NIST, as well as the industry, to work together to try to be as responsive, to look at the vulnerabilities, to intercept them in advance. We work with the other Federal agencies to do that as well.

Mr. DAVIS. Mr. Wolf, what is your thinking on this, on the standards and are they needed and in what direction should they be developed?

Mr. WOLF. I think standards are very, very important. We need to make sure we cover the waterfront in terms of all the areas that need the standards and I think my partner on the committee here mentioned some of those. We need to make sure they get implemented. I think that is probably one of the toughest things in terms of standards out there, do people actually make use of it? And it goes along with the assessment that you have in your bill where you talk about the assessments, where you are actually doing security assessment. If you have a set of standards, how do you make sure people are actually implementing them? How do you do an assessment to see that is happening? And how do you do the reporting to make sure that happens?

We look at various hacking incidents we see in FedCIRC and in many cases, it is because people haven't implemented standards, haven't implemented patches, things like that.

Mr. HORN. It was mentioned earlier that the encryption would require greater standards than others. What would be the difference between a domestic agency and an intelligence foreign affairs agency, would it make much difference in terms of what NIST is going to undertake which is various types of standards, could that be used to cross areas? How many simple standards are there that go across the whole executive branch?

Mr. WOLF. I would say there are certainly things NIST is doing that apply across the Government. There are probably some addi-

tional things you would want to do in the national security arena that are probably a little stricter, because of the nature of the data being handled, the Internet connections, the internetting, things like that.

Mr. HORN. That makes some common sense. Do you believe we should continue to manage national security systems separately from the Federal information systems?

Mr. WOLF. I think you need to set a set of standards, I think they need to be comprehensive but in some cases, when you are talking national security, there may be reasons why they cannot be implemented because of the national security environment in terms of what we are doing. So I think there are some distinctions there. Standards are important, they need to be comprehensive but not necessarily dictating they are always used. There needs to be that case, where because of national security, there is a reason you are not going to implement them and maybe you propose an alternate set of standards for the national security which may be stricter or may have some differences because of national security environment.

Mr. HORN. What interests me is can we keep this going with OMB having the responsibility on behalf of the President and we are not looking for jobs up here on Capitol Hill, we have plenty to do. The question will be how do we know and how do inspectors general, in particular, know when they are being sandbagged within a particular agency because nobody can talk to them?

Mr. WOLF. I am afraid I am not qualified to answer that question. In terms of the role NSA has in terms of defining what are good security practices across the board, we are very active with NIST in those. In terms of enforcing those in various government agencies, we are not able to do that. We certainly can define what they should be.

Mr. HORN. Mr. Forman, is the best way to see if the CIA is going along with the type of security situation and to take a look at it of either leaving it to the Inspector General at CIA or you are going to do it? Or do you just turn NSA loose on them to see they really have done what OMB would want so you don't have another Ames or whatever? There ought to have been a lot of things that they haven't done.

Mr. FORMAN. While I am always loathe to recommend more bureaucracy, I think this is an area where we want to make sure we are taking a good, cost-effective approach, but we ought to err on the side of risk-diversity. We are forever hearing terms about standards in areas where, technically, they don't mean the same thing as a standard.

We recently produced, last November, the advanced encryption standard, which is a product of NIST but really a product as much as any of the standards we have, leading edge, a function of where industry is going, the national security community, and civilian agencies. It is a fine standard, a technology standard.

I differentiate that from saying what is our standard for middle ware or what is our standard for a Web applications server. Those are more what I would consider to be components. The nexus that we have there, the process that we are rolling out, combines the CIO Architecture Committee, which I think you will see, have an

increasingly important role in terms of understanding and agreeing to the architecture components, and there is now in circulation a framework for doing that.

I think Ron's role as the CIO Council Security Liaison, integrating within the Cyber Board executive branch committee which NSA also sits as a member, is another critical part of that puzzle, pulling together the key issues to focus.

So we know we will have that focusing, we will get that more rapid approach to different types of standards as well as the architecture components. The next step then is how do you police that? We will do some by the budget process, and I think that is key, but there is a set of analytical capabilities as Ron mentioned, that center for excellence, that also has to focus the audit work, inform and accelerate that standard setting process.

I think as you heard before, there is some good language in FISMA, and I think the suggestions in the testimony and answers to the questions will focus that a bit more. At the end of the day, I think you are looking at a couple of key elements here, how fast can we make this process work and some end results. Not only are we seeing increased vulnerabilities because those are going to increase just because we are detecting more, but are you seeing people taking advantage or hackers taking advantage of those both within, the internal threat, and the external threat in a way that causes mission critical problems, loss of privacy.

I think the bill should lay out very clearly what are the criteria, what are the results that will measure? Is it loss of privacy? I think that is a fine one, it is in some of the legislation already and it would be good to focus it in FISMA. Is there loss of mission critical capability or downtime? If you lay out the guidance and the measures I think that will help us in focusing the oversight and the standard setting process through components.

Mr. HORN. Mr. Dacey, what does the General Accounting Office think about the various standards that might be put forth under this bill? The question is, does it help with doing it or if it isn't, why even have it?

Mr. DACEY. We think standards are important. I think one of the challenges to your original question is to provide some level of standardization but yet build in sufficient flexibility to make sure we don't make bad decisions and put in things we don't really need. I think that will be the challenge in implementing it.

I think there are a couple of things I would like to focus on here. In FISMA, it sets up a requirement which is general good practice, that you should assess your risk and develop security controls commensurate with that risk. As part of that process, FISMA then goes on to establish a requirement for risk levels and standards for those various risk levels. Let me talk briefly about risk levels and standards.

In terms of the risk levels, it is clear and it has been said on the panel here, we really need to have an effective and efficient process for assessing risk. It is a very important aspect because if we don't do that properly, we are not going to have the right controls in place to protect our systems.

It is also important to consider how you go about doing that. FISMA comes up with levels of risk. That could be a very feasible

approach I think to categorizing the types of risks and systems and the various ways you could build that around. I think that would be part of the deliberative process to consider how those would best be established.

I think they are important too when we talk about connectivity because we are talking about right now pretty broad spread connectivity within agencies, between agencies, between the Federal Government and State and local and with the private sector. I think ultimately we need to be considering what is the level of risk in those systems and do we want to have them connected together. That would be one way which this could go through the process.

You wouldn't want to be connecting openly a high risk system with a low risk system because a low risk system would have less safeguards and those safeguards could potentially be breached and gain access to the more sensitive system and that is typically what we do when we do our work in trying to get into Federal systems with the agency's knowledge. We get into systems that are simple to get into and use that ability to advance our privileges and gain access to some very sensitive information.

In terms of standards, I think there may be some definitional issues. One of the concerns is the word standard oftentimes evokes a certain amount of rigidity or inflexibility. I don't think that should be the intent of standards under FISMA. I have been doing auditing for about 25 years and we use auditing standards. I audited small shops, I have audited the Federal Government with its $2 trillion of revenue. We use the same standards, not the same procedures but the same standards nonetheless and it has worked pretty well and it is generally applicable. That is the kind of standard I think I would refer to.

I think they are important for several reasons. I think they clarify expectations. I think they are a good criteria to measure how effective security is, as well as to manage performance or measure performance over time. I think it provides a certain consistency if we have standard levels of risk, that we have some nomenclature to share within the Federal Government as well as those we choose to hook up to our systems as to what level of risk we want them to respond to. In fact, in some of our more secure systems, there are requirements before you hook up to the systems. You have to meet certain minimum security requirements or you don't play the game. I think there are some examples already where that is being used to say we need certain standards to deal with that.

GAO's approach has to address all these. When we do our audits, there aren't universal, governmentwide standards necessarily and that is a challenge to us. But what we find oftentimes is that there is a core set of standards or requirements that are pretty universally agreed upon. I don't think we have found anyone who said if you are going to have passwords, you probably ought to say fault passwords should be removed because everybody knows what they are and if they get in the system, they can break right in.

Also, you could argue that maybe you shouldn't have passwords if you are going to use passwords to say "Redskins" or "password" as the password. Those are the types of things in which I think there is a lot of agreement. There are probably some other stand-

ards that there is some reasonable difference between knowledgeable people as to whether it should be a requirement or not. I think that could be considered again in the structure of a standard-setting process.

I think there are some other side-benefits to standards. I think if we are going to have some consistent training across the Federal Government, which I think is one of the goals of the administration, I think it is a very important goal to the extent you have some standards to build that around. To be training people on the same thing would be very important.

We also have a lot of people running these systems that have worked very hard and to the extent you can provide them some information rather than have them independently try to determine what level of security they should employ would be beneficial.

Last, in terms of tools, I think that is another important area, we need better automated tools. Many of those tools currently look for certain things in the systems. I think if you agree upon what those things are you want to look at, tools can be built rather readily to test for those types of conditions in those systems.

Mr. HORN. We look on the General Accounting Office to be the sort of umpire on behalf of Congress. What are the benefits and disadvantages of shifting responsibility for promulgating standards and moving it from the Secretary of Commerce to the Director of Office of Management and Budget? How do you feel about that one?

Mr. DACEY. If you go back in terms of prior legislation, there certainly has been the involvement of both NIST and OMB in development of standards and oversight of responsibilities for those standards' I think starting with the Computer Security Act and going on. What FISMA would do would be to align those responsibilities with OMB, who is directly responsible for the oversight and coordination of the agency information security. That is where it would place that. I think that is a good matter for discussion. Obviously we have some differing views and I think that ought to be considered in any final legislation.

Mr. WU. As I mentioned in my opening statement, we believe that should be a matter for reconsideration. The Director of OMB issues broad information security policy and guidelines to agencies complemented by detailed security standards and guidelines which NIST develops.

The proposed process presents an opportunity for delay as additional senior managerial approvals are going to be required up the bureaucracy. As we fight the war on terrorism, we believe we should be thinking about how to streamline the development and issuance of new security standards while still maintaining the important process of public review and comment. Since NIST activities are more directly linked to industry and the Secretary of Commerce represents business and industry and commerce, we believe it is more appropriate for that role to remain with the Secretary and not with OMB.

Mr. HORN. What criteria would you use to determine if a standard is mandatory or non-mandatory? How would you go about that?

Mr. WU. Quite frankly, I am not sure how we are going to make that determination but we would have a plan in place. I don't think

it is necessarily going to be a uniform determination but done more on an ad hoc basis, in consultation with the experts and our cyber security team.

Mr. FORMAN. Mr. Chairman, the process we have laid out in my prepared statement with the cyber boards, executive branch committee, lays it out, a cost-benefit, risk-based approach, very similar to how one might say you should insure yourself because that is in essence what we are trying to achieve here. So cost-benefits, risks, specifics of that situation, I think is what is going to drive that determination, certainly the guidance that cyber board will provide to NIST and NIST supporting us on that board.

Mr. HORN. Can you provide, Mr. Wu, an example of a minimum standard the National Institute of Standards and Technology would make mandatory?

Mr. WU. As I said, I am not clear as to the determination on what would be defined as mandatory. We can get back to you on that in consultation with our cyber security team.

Mr. HORN. One would be the password to get at the basic machine or the software or whatever. Then the question, what kind of watching does the control authority, OMB and you, partially in that, and that would be it seems to me one of the obvious.

Mr. WU. That would be one but I don't have a definitive list for you. We can try to provide that for you if you like and to the committee.

Mr. HORN. I understand that NIST has developed mandatory standards in the area of cryptography. What has been your experience in implementing those standards within the Federal agency? Have you developed mandatory standards in other areas or just in the ones with encryption?

Mr. WU. Right now, my understanding is that it is only with encryption. We have had a lot of success working with OMB and the other agencies with AES, advanced encryption standard. We look forward to continuing with that collaboration under that framework and structure.

Mr. HORN. Is the 1988 Secretary of Commerce delegation of authority to waive Federal information processing standards to the agency still in effect?

Mr. WU. I personally don't know that answer but we can get back to you.

Mr. HORN. We will put it in the record at this point.

Mr. WU. I have been told the answer is yes.

Mr. HORN. That it has waived Federal information processing standards to the agency heads and that is still in effect. OK.

The problem often comes up over time, like 100 years, that it is very difficult for a member of the Cabinet to work with his other members of the Cabinet and they will listen to OMB and might not listen to good old Joe or Susie who are doing something. That is one of the things we look at and wonder who will do what.

Mr. Forman, what type of standards and guidelines has the CIO Council developed?

Mr. FORMAN. Let me differentiate standards versus guidelines. The CIO Council was established by Executive Order, it is not created in statute. The Executive Order has OMB as the Chair of the council and directs the council to provide recommendations and ad-

vice to OMB on IT issues and that the members share best practices across the agencies. It really has had no policy guidance or standard setting authority.

In that regard, one of the changes I put in place being the Director of the Council is to actually get them focused on some standardized processes or procedures or approaches. Let me give you some examples and then I will talk about security. Let us refer to these as guidelines to make it clear.

One is the Enterprise Architecture Management System, a tool that was developed for tracking and leveraging the component based framework we have been deploying.

The second is the Federal Enterprise Architecture Framework. Basically, this is the way now that we back up with a scorecard and the budgeting process to get agencies to clearly identify the linkage between their IT investment and the mission of the agencies driving through to business cases.

There is a corollary tool to that, ITIPS, the IT Investment Portfolio System. Now each agency is supposed to use and put in place a capital planning process. This is a tool and between those two tools that are the guidelines laid out by the CIO Council, we are now able to get the information in and start to analyze the architecture we have built in the Federal Government. We are not to the point where we can define it yet.

The Federal Enterprise Architecture Framework document is getting to that point. We have laid in terms of a governance structure with that is a role for the Architecture Committee. They will come to agreement on components, this approach is essentially the CIO's all coming agreement and they are doing it for a number of reasons, not the least of which is money, leveraging their investments to get more out of industry by moving those component points, to be able to take advantage of Web services and some of those are emerging in the security arena.

The fourth area I would say we have a decent example of a guideline is in the work force training arena. Security is a key component of that. I think the CIO Council training components and the framework laid out for CIO University Center is widely regarded even in industry. We see more industry take up of that agenda than government employees.

Those are the types of things that are appropriate. We are leveraging NIST very highly in the security arena. For example, taking the benchmarking or the analytical guidelines, I wouldn't quite call those standards that were developed over the last year, and that serves—and everybody has agreed to use that—as the basis for the GISRA work. It allows us a standardized approach if you will, but not the same as the Federal information processing standards which are technical standards.

Mr. HORN. What types of standards and guidelines has the Chief Information Officer Council developed and if so, do they go through OMB primarily to get those functions across or do they have any authority to spread the guidelines, if you will?

Mr. FORMAN. They do refer them to OMB and we work, like in those four examples, by incorporating those into two basic OMB circulars. We can obviously issue other guidance, but the predominant way you will see this is through the A–11 Circular and the

A–130 Circular. Again, that is what I would consider guidance or guidelines as opposed to standards.

I think you will see this get integrated much quicker by the CIOs agreeing to those architecture components and going back and putting that into their architecture. We will see that through their IT investments and the architecture results they have to submit to OMB but at the end of the day, this is about managing change. What we are seeing, I believe, is formalizing the Clinger-Cohen approach on the roles and responsibility of the CIOs.

I will give you an example of what I am talking about. As you know, we have an issue in the Justice Department on leveraging the technology to make the management changes. Recently they hired a very well qualified CIO and made that person a direct report to the Attorney General with the full fledged authorities, architecture included, laid out under the Clinger-Cohen Act.

So coming to agreement using the technology insight from both NSA and NIST, the results coming out of the Cyber Board Executive Committee, firming up those agreements by that Architecture Committee, and then we provide the oversight to make sure when we review the architecture and the business cases that indeed they are complying to those guidelines.

Mr. HORN. The current bill removes OMB specific authority to approve agency security plans. Do you believe that authority should be restored?

Mr. FORMAN. I think, as I understand the bill and what is currently in GISRA, is the approval of the security programs and we have to differentiate between the security programs and the plan of actions and milestones. There, I think, is actually where the Director of OMB should focus. We know and are getting terrific insight from the IGs, from the reviews GAO is doing and our strong relationship there, and indeed from some of the CIOs' risk assessments.

To have us prove the fact that there was a problem, I don't think gets us anywhere. The focus on approving the plans of action and milestones is the appropriate approach and I think that is what is laid out in the bill.

Mr. HORN. With GISRA, with expiring in November of this year, and the OMB estimating that the fiscal year 2003 funding for the information security will be $4.2 billion, is it reasonable to expect the Congress to wait until September or later to learn whether agencies are taking the appropriate corrective actions to address their information security weaknesses?

Mr. FORMAN. I think it is really a question of the oversight and governance structure you have. I think what we are moving to with your subcommittee is a quarterly review of our progress. That is certainly the approach we have moved to in OMB. The approach I am going to adhere to is a quarterly review of agency progress.

Mr. HORN. That is when we went through the Y2K bit, that is exactly where we got and went to. It started out with almost once a year and then to two times a year and then Dr. Raines in particular understood all this and we got to quarterly. I think that makes sense so everybody knows we want to look in that quarterly operation because Congress might look at it.

How does the committee, Mr. Wolf, the Committee on National Security Systems which has set minimum standards for the protection of national security systems and if so, what is your experience in implementing these requirements?

Mr. WOLF. I think the committee has been very active since it was formed. It replaces one of the earlier committees that started in 1990. There are over about 100 policies that have been issued; some of those include some standards. The standards I think are fairly rigorously enforced in the national security environment, so I think it has been very effective. I think it has addressed many areas where standards are needed, been very active. So I think it has been very successful.

In terms of looking at some of the policies, the rest of the Federal Government might look at some of those policies as at least a start in terms of policies in some areas where they might not have been addressed so far.

Mr. HORN. Has the National Security Agency developed a standard for risk assessments and management that is used for national security systems?

Mr. WOLF. We have some templates. I am not sure to the detail that we have those developed but we have some templates that we use. There is I believe a DOD standard also.

Mr. HORN. How did NSA approach the evaluations of national security systems under the Government Information Security Reform Act? How has it gone?

Mr. WOLF. I am not sure I can answer that question. We will have to get back to you on that one. Again, our role is sort of an advisor in the agency. We are not the actual agency that does that evaluation.

Mr. HORN. OK. What guidance did NSA provide to agencies with national security systems? Did NSA work with the Director of Central Intelligence to coordinate evaluations or guidance for the evaluation of intelligence systems?

Mr. WOLF. We certainly are given input, yet, again, as an advisor.

Mr. HORN. It is the Director of CIO that has that authority?

Mr. WOLF. Yes.

Mr. HORN. Let me ask you, Mr. Miller, about FEMA. You recommend that the bill be revised to strengthen the link between IT security requirements and the capital planning process. What specific revisions to the bill would you recommend to strengthen the link between them?

Mr. MILLER. First of all, OMB has taken some steps to ensure that when we do our funding documents, our 300-Bs, that there is a security tie to it. I think tying the approval of IT spending to a demonstrable security plan, not just saying we are going to spend money on security but actually having a plan you can demonstrate you have processes and procedures in place, would be a powerful incentive because from the CIO perspective, we have to persuade our program officials, the folks actually benefiting from these systems, that there is a reason why security should be factored into their equations.

Within FEMA, we are trying to implement a process by which we don't spend a dime or allocate a person or time to a project until

they have addressed the security issue among others. That process has caused a lot of interesting responses but we believe it is the right thing to do.

The key there is to make sure that people just don't pay lip service to security and the 300-Bs, that they can actually demonstrate there is someone thing behind it when they say they are addressing security.

Mr. HORN. Mr. Williams, in your role as an Inspector General, what challenges do the IGs face in integrating an annual independent evaluation into their audit workload?

Mr. WILLIAMS. As with anything, the prototype consumed about three or four times the amount it will on an annual basis. I don't know that it was a great difficulty for the IGs. It was certainly something that we were pleased to see come and we appreciated the role that we played.

It is very important that we stay in touch with the advances and challenges on the security side. This is a role that allows us to do that without being overly intrusive. It is an important part of the entire process in GISRA. I think it is one we embrace. Where there is need for advanced or temporary skills, we can get that through contractors as the department does as well.

Beyond that, I don't know that it represents any sort of formidable challenge. I think it has been something we have appreciated.

Mr. HORN. Mr. Dempsey, you suggest as an interim measure that agencies should adopt a widely accepted set of standards developed by the private sector. Can you provide some examples of those?

Mr. DEMPSEY. It takes me a little bit outside my direct area of expertise, I have to admit. I know that there is the so-called common criteria standards which have been developed that address computer security issues. I think that there are others in industry who are much more familiar with those than I. I can certainly flesh that out for you and give you some examples of work that has been done in the private sector that would contribute to the Government's efforts.

Mr. HORN. We would welcome those.

Mr. Dempsey. We have to do so.

Mr. HORN. I want to put in the statement of the ranking member, Ms. Schakowsky at the opening and we will put that after Mr. Davis' opening.

She has two points here that I think are very important. She says, "There does seem to be one significant hole in this legislation. As we learned in confronting the Y2K problem, we cannot be sure all of the systems are fixed until we know where they all are. The first thing most agencies had to do to prepare for the turn of the millennium was to create an inventory of all computer systems and then assess the risk posed by the failure of each of those systems. It is a commentary on computer security that no such inventory existed." Is that correct?

Mr. FORMAN. That is the corollary on why the CIO Council was adopted the enterprise architecture management system to build that inventory.

Mr. HORN. She says, "When we mark up the bill"—Mr. Davis might want to listen to this—"I intend to offer an amendment that

would first require all agencies to maintain a current inventory of systems. Second, I will require that agencies develop and include in the security report a plan that establishes a system whereby every system will be tested over a 5-year period. With a current inventory and scheduled testing, we will be closer to security being a routine and not a unique government function." I think those are pretty good comments.

Let us go right down the line with your thinking about that.

Mr. WOLF. I would add one comment. It is not only the inventory of all those systems, but it is how they are interconnected and whether or not they have implemented the standards and what standards they have implemented so you know what you are really talking to.

We have a very active red team and you rattle the windows of a house and you only have to find one window that is open and that is the one place where they haven't implemented the standard or put in the patch. It is not only an inventory of all systems, but how they are interconnected and what they have done in terms of standards.

Mr. WILLIAMS. Probably an emerging area that ought to also be considered is a corollary, the establishment of new gateways. We are discovering that some of the gateways are not to expand the e-government and other kinds of good initiatives. They are not always apprising the CIO of the existence of the gateway and the gateways aren't always being tested for intrusions and vulnerabilities.

I think the point the Congresswoman makes is a good one but I would add that to it as well. That is probably the one where we have seen most recent vulnerabilities emerging.

Mr. MILLER. I want to second what he said because I think it is very important. Awareness is where we begin in the area of security and just as an example, in our agency we discovered during a vulnerability assessment that we had over 500 servers in an agency of 2,500 people. We weren't aware of them, so right away we have all these potential entry points to our network that we didn't know about.

We have initiated an audit of all FEMAs IT assets and that starts this month and goes until we find everything. Key to that is having our Director's full support which he has given us, so we won't have people trying to hide things under their desks. We will find them and once we know where they are, we can start the process of holding people accountable for them in the area of security.

Mr. WU. As you alluded, the success of Y2K wasn't just that we battled back the Millennium Bug but also that we were able to engage in the first ever exercise in which we had a Federal inventory of our IT infrastructure. This was also being replicated in the private sector as well.

The inventory is only the first step of trying to assess what our critical needs are and what the demands are. I think the inventory could prove to be very useful.

Mr. HORN. I agree with you completely. The fact was we asked that the hardware and the software be inventoried if you are going to come up to the Congress for money and you deserve to have it in a lot of those agencies. I would think that would be worth doing.

We did have a list that was put together by a lot of the CIOs and when Mr. Gingrich was here as Speaker, he was quite interested in this sort of thing, so we were able to give the appropriators the "go" signal which is green up here as opposed to some systems I have seen where the Xerox just doesn't give a nice color to it. I think that is what we need if we are going to solve some of this problem. It is going to take money and hopefully we will get that going.

I now yield to the gentleman from northern Virginia and the world across the Potomac. He has a great bill here. Any questions you to ask?

Mr. DAVIS. No, I think I am OK. I really appreciate the panel coming today and sharing your observations. I hope we can make it a better bill and I think between Chairman Horn, myself and the leadership, we intend to move this pretty quickly. We would look forward to any additional input you can offer.

Mr. HORN. I want to thank the subcommittees involved in this. In back of me is J. Russell George, staff director and chief counsel for our subcommittee. He is a nominee of the President of the United States to be a fellow IG, you might see him, but first we have to get him confirmed. He has been a great leader in this for years now.

Also, Bonnie Heald, deputy staff director and communications director. On my left is a very able person, Claire, who is our professional staff on loan from the American Political Science Association, and has done a wonderful job. Henry Wray, I think most of you know, our senior counsel, worked with the Senate and we tied him up, got him across the Rotunda and he now works for us, and he is doing a great job. Then Earl Pierce, professional staff, and Justin Paulhamus is the majority clerk.

We thank today the court reporters, Mary Ross, and with Mr. Davis, you have Chip Nottingham and Teddy Kidd from the Subcommittee on Technology and Procurement Policy.

We thank them all.

Gentlemen, I appreciate what you put on the record today. Keep at it.

[Whereupon, at 12 p.m., the subcommittee was adjourned, to reconvene at the call of the Chair.]

[The prepared statement of Hon. Janice D. Schakowsky and additional information submitted for the hearing record follows:]

STATEMENT OF THE HONORABLE JAN SCHAKOWSKY
ON H.R. 3844
THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT

May 2, 2002

Thank you Mr. Chairman. This is our fourth hearing on computer security in this Congress, and the message has been uniformly dismal. Agencies are not doing the basic tasks necessary to protect government computer systems.

Most of our witnesses have told us the same story. Computer security is not rocket science; it is performing some basic functions repeatedly and consistently. We have all heard witnesses testify about basic functions like changing the password when installing new software, and programs that force users to routinely change their password, go a long way towards improving security.

Unfortunately, management has not made security a priority, and as a result, it has not been a priority for the staff. The Government Information Security Reform bill was an attempt to make security a priority for management. It was a step in the right direction, and the bill before us today is a substantial improvement.

H.R. 3844 requires the same agency security reports and Inspector General reports that the Subcommittee used in grading the agencies last fall. Now we must assure that Congress has access to those reports.

H.R. 3844 improves upon past legislation by bringing the National Institute of Standards and Technology into the process. This bill requires an agency to assess the risk associated with its systems, and requires NIST to provide the agencies with guidance on the best way to secure against those risks.

There does seem to be one significant hole in this legislation. As we learned in confronting the Y2K problem, we can't be sure all of the systems are fixed until we know where they all are. The first thing most agencies had to do to prepare for the turn of the millennium was to create an inventory of all computer systems, and then to assess the risk posed by the failure of each of those systems. It is a commentary on computer security that no such inventory existed.

The same situation applies to security. Before an agency can determine its risks, it must first create an inventory of all systems. Very few agencies have kept the inventory current.

When we mark up this bill, I intend to offer an amendment that would first, require all agencies to maintain a current inventory of systems. Second, I will require that agencies develop and include in the security report, a plan that establishes a system whereby every system will be tested over a five year period. With a current inventory and scheduled testing, we will be closer to security being a routine and not a unique government function.

Again, thank you Chairman Horn for your persistence in keeping computer security on our agenda. It is a dry and arcane subject, and all too often we let those issues slide. Your diligence is a valuable service to Congress and to the administration.

UNITED STATES DEPARTMENT OF COMMERCE
The Under Secretary for Technology
Washington, D.C. 20230

Response of

Benjamin H. Wu
Deputy Under Secretary for Technology
U.S. Department of Commerce

To the
Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations
House Committee on Government Reform
Re: May 2, 2002

Q: An example of a minimum standard that NIST would make mandatory (and how would you determine what should be a minimum standard).

A: The following are examples of the types of minimum security requirements NIST would recommend be made mandatory for federal agencies:

Security awareness and training program

- Agencies shall train employees, contractors or other third parties (with physical and/or logical access to IT systems) on security policy/objectives specific to the overall organization, their specific responsibilities, and security procedures.
- Training shall be conducted at least annually.

Personnel security controls (background checks, duties, position risk designations, etc.)

- Agencies shall designate positions to the level of security risk they present to the agency's mission.
- Agencies shall institute a formal program of screening and background checks for employees, contractors or other third parties who may carry out designated functions in support of the organization commensurate with the agency's determination of a position's sensitivity.

Firewalls

Agencies shall employ firewalls to protect their network domain from other domains not under the agency's full control but which interface with its infrastructure to help protect against intrusion attacks via the INTERNET, virus attacks and malicious active content.

System patches

Agencies shall implement a program to ensure that patches are applied as soon as possible, with the systems at greatest risk addressed first. (*Note: Analysis of impact on*

other software interfacing with/dependent upon the system software where patch is to be applied must be factored into the patch application scheduling by agencies).

Virus detection/eradication/containment

- Agencies shall implement virus protection on all servers, workstations, and mobile computing.
- Virus protection employed by agencies shall include a capability for automatic updates.
- Updates shall be conducted at least weekly.

Validated cryptography

Agencies shall only use cryptographic products and services that have been successfully validated under NIST's Cryptographic Module Validation Program. (Note also that there currently are mandatory technical standards for government agencies when they determine they need to use cryptography (as opposed to another method) to protect their information. These standards include Federal Information Processing Standard 140-2, "Security Requirements for Cryptographic Modules" and FIPS 186-2, the Digital Signature Standard." When agencies need to use encryption, they must use one of three approved algorithms as specified in FIPS 46-3, "Data Encryption Standard," FIPS 185, Escrowed Encryption Standard," or FIPS 197, "Advanced Encryption Standard.")

> *N.B.: Note that the examples above may often be supplemented with guidelines and additional detail.*

NIST envisions creating minimum requirements of the type specified above for *all* systems to provide basic-level protection. For systems with medium or high security requirements for confidentiality, availability, and/or integrity, NIST would specify increasingly strict requirements.

In developing these minimums, NIST plans to develop a draft proposal and seek comments from agency security officials, Chief Information Officers, the Computer System Security and Privacy Advisory Board, and other interested/affected parties and to work as appropriate through the Executive Branch Information Systems Security Committee.

STATEMENT FOR THE RECORD

BY

Sallie McDonald

Assistant Commissioner,

Information Assurance and Critical Infrastructure Protection

Mr. Chairman and Members of the Committee. On behalf of the Federal Technology Service of the General Services Administration let me thank you for this opportunity to discuss GSA's office of Information Assurance and Critical Infrastructure Protection role in Federal Information Security. I want to express my appreciation for your interest in the Information Security of the Federal Government. **Although I am not in a position to express the Administration's views on H.R. 3844, the 'Federal Information Security Management Act of 2002,' I thought it would be useful to share GSA's experience with the Subcommittee** and discuss how my organization can help to implement the vision articulated in the proposed legislation.

Background

The Office of Information Assurance and Critical Infrastructure Protection is home to the General Services Administration, Federal Technology Service's Federal Computer Incident Response Center, (FedCIRC). To meet the requirements of OMB policy, the National Institute for Standards and Technology (NIST) developed FedCIRC in 1996 as a pilot program. It became operational in 1998 and was moved to GSA's Federal Technology Service. The overarching mission of the FedCIRC is to be the Federal Civilian Government's trusted focal point for computer security incident reporting,

sharing information on common vulnerabilities, and to provide assistance with incident prevention and response.

FedCIRC was designated by the Office of Management and Budget, and subsequently by the Government Information Security Reform Act (GISRA) as the Federal Civilian Government's central reporting entity for computer security incidents and sharing information on common vulnerabilities. We maintain a 24x7x365 security operations center to handle incident reports from across the Federal Government. These reports come in via our toll-free telephone number, electronically through a form found on our web-site, via email, and via both secure and unclassified fax. This enables FedCIRC to assist agencies in recognizing the nature of an incident, and also permits us to identify when an incident might be part of a larger, coordinated attack on Federal information systems.

The FedCIRC is more than just response. We take special care to stay informed of the latest vulnerabilities and threats to the hardware and software systems on which so many vital government services depend. We have processes and procedures to rapidly inform agencies of emerging threats and vulnerabilities, and to explain steps that can be taken to reduce the risk and mitigate the threat. We provide tools to help Federal information security professionals identify vulnerable equipment on their networks, and to help them take steps to correct the problems.

FedCIRC does not attempt to achieve this in isolation. We are part of an active information-sharing community including the Department of Defense, the Intelligence Community, Law Enforcement, Industry, and Academia. We are currently leading an interagency working group in support of the President's Critical Infrastructure Protection

Board to develop a more thorough understanding of the threat and potential corrective measures to address a newly identified, widespread software vulnerability.

Additionally, since each Federal agency has different expertise and strengths, we chair an ongoing forum of Federal Incident Response Teams. Known as the "FedCIRC Partners Group," these dedicated computer security professionals meet quarterly, and share information continually through email. This fosters an increased level of trust across agency boundaries, and establishes an informal network of experts who can rapidly conduct assessments and share their understanding of emerging threats.

Discussion

The Federal Information Security Management Act calls for the creation of a Federal Information Security Incident Center that would provide a single point of contact for Federal civilian agencies to report incidents. The development and operation of this center is to be overseen by the Director, Office of Management and Budget. The center is to provide timely technical assistance to operators of agency information systems regarding security incidents, including guidance on detecting and handling information security incidents. Additional responsibilities include: to compile and analyze information about incidents that threaten information security; to inform operators of agency information systems about current and potential information security threats and vulnerabilities; and to consult with agencies or offices operating or exercising control of national security systems.

The FedCIRC currently does all this and more. Permit me to address each point individually, and then to share with you some of the initiatives we are implementing,

based on the three and a half years experience we have gained filling this role for the Federal government.

Director, OMB oversee the development and operation of a Federal information security incident center. In its memorandum M-01-08 dated January 16, 2001, the Director, Office of Management and Budget reinforces existing policy requiring agencies to develop plans to report incidents to FedCIRC. FedCIRC has been assisting Federal civilian agencies with their incident handling since October 1998. Additionally, a senior advisory council meets quarterly to discuss FedCIRC's goals, accomplishments, opportunities and progress. This council includes senior representatives from OMB, GSA, the CIO Council, NIST, the Department of Defense, the National Security Agency (NSA), the National Infrastructure Protection Center (NIPC), and Academia (represented by Carnegie Mellon University's CERT®-CC).

Provide timely technical assistance to operators of agency information systems regarding security incidents, including guidance on detecting and handling information security incidents. FedCIRC's principal area of focus is to provide timely technical assistance to the Federal civilian government agencies. FedCIRC has been working closely with individual agencies to develop the trust and confidence needed to implement the stated purpose of FISMA: to contribute directly and significantly to "a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets." This trust must be earned through proven performance and success. FedCIRC has done much to develop this trust.

One example is in the Federal government's handling of the "Code Red" virus that infected millions of systems worldwide in the summer of 2001. Code Red conducted automated network scanning to identify systems operating with a vulnerable server software package. A public advisory had been previously released identifying a serious security vulnerability that could allow an intruder to gain control of the vulnerable system and employ it to scan and infect other vulnerable systems. The first version of Code Red commanded thousands of infected computers to simultaneously flood the White House web site, which would result in a denial of service, denying access to citizens seeking legitimate information from the White House web site. The attack was thwarted in part by changing the internet address of the White House web server. This action redirected the attack against a non-existent address, negating any service impact.

Industry and government experts quickly reached a consensus that the rapid rate of infection, and resultant volume of automated scanning posed a threat to the Internet infrastructure's ability to process the extremely high volume of traffic. A tool was made available to help identify vulnerable equipment, and a patch was created to correct the vulnerability. FedCIRC provided the tool to government agencies and ensured that agencies had access to the corrective patch. OMB required agencies to report to FedCIRC when their vulnerable systems were patched. As a result of this decisive action, the impact to the government of Code Red and its later variants was minimized.

Compile and analyze information about incidents that threaten information security.

FedCIRC is currently the Federal civilian government's point of contact for compiling and analyzing information about incidents that threaten information security. Agencies recognize the FedCIRC as providing this significant service. FedCIRC has developed

trust relationships during the past three years necessary to provide such services. FedCIRC employs the services of Carnegie Mellon University's CERT®-CC to conduct detailed research and analysis. CERT®-CC was created in 1988 to performs a similar function for DoD after the infamous Morris Worm brought down what was the predecessor of the Internet. Their unique position as a Federally Funded Research and Development Center permits CERT®-CC to analyze information about computer incidents from both the Civil and Defense agencies of the Federal government, and to combine that analysis with a wealth of knowledge gained as the academic community's leading computer security research center. In cooperation with CERT®-CC, FedCIRC has implemented a process to disseminate special notices, alerts and advisories, based on this analysis.

Inform operators of agency information systems about current and potential information security threats and vulnerabilities. FedCIRC continues to partner within the Federal government and out into industry and academia to provide sophisticated data back to agencies on threats and vulnerabilities. FedCIRC has developed numerous programs and services for the agencies – all at no cost to agencies. Lately these include discussions on significant vulnerabilities via conference calls with industry experts and CIOs, email alerts, and workshops.

In March 2002 we implemented a contract to provide a security Patch Authentication and Dissemination service. Operational in June, this service will provide a process in which operators of agency information systems will receive notification of vulnerabilities affecting the systems they employ. When patches are developed to correct these vulnerabilities, FedCIRC will authenticate the patch to verify that it does indeed correct

the vulnerability. We will then advise Federal operators on how to access the patch, and how best to implement it. If a patch is not yet available to correct the vulnerability, FedCIRC will provide advice on steps to reduce the risk. This is the first service of its kind to leverage on vulnerability notification services, combined with testing and authentication of vendor and manufacturer patches, and FedCIRC has received a great deal of interest in this service from our Federal civilian constituency as well as DoD, and State and local governments.

Consult with agencies or offices operating or exercising control of national security systems. FedCIRC has created multiple processes to consult on a regular basis with multiple centers of expertise in government. FedCIRC's programs have lead to significant partnerships across communities that are traditionally stovepiped. FedCIRC is in daily contact with DoD's Joint Task Force for Computer Network Operations (JTF-CNO), the National Infrastructure Protection Center, and NSA's National Security Incident Response Center (NSIRC) which also hosts the Intelligence Community Incint Response Center (ICIRC). These daily conference calls facilitate sharing of information affecting computer systems across community boundaries. In addition to routine daily calls, this partnership facilitates the trust necessary to foster true collaboration in the event of intentional threats to US Government information systems. This collaborative effort has resulted in the development of a virtual incident response community. Though the respective missions of these organizations vary in scope and responsibility, this virtual network enables the Federal Government to capitalize on each organization's strategic positioning within the national infrastructure and on each organization's unique access to a variety of information sources. Each entity has a different, but mutually

supportive mission and focus which enables the incident response community to simultaneously obtain information from, and provide assistance to Federal agencies, DoD, the intelligence community, industry and academia.

FedCIRC, NIPC, NSIRC and JTF-CNO are involved in a constant sharing of sensitive cyber-threat and incident data, correlating it with counter-terrorism and intelligence reports to develop strategic defenses, threat predictions and timely alerts. These efforts depend not on any one participant, but on the unique and valuable contributes of each organization. Alerts and advisories are frequently generated by this group, and represent a consensus when distributed to Federal agencies, industry and the general public.

Summary

The vision articulated in H.R. 3844 is one that GSA shares and supports, wholeheartedly. This vision is completely in concert with the mission of the Federal Computer Incident Response Center. FedCIRC already provides each of the services required in the proposed statute for the "Federal information security incident center." The FedCIRC is more than a physical office. During the past three and a half years, the FedCIRC has created multiple processes that bridge across the Federal government and industry – which owns most of the cyber infrastructure and shares selectively with trusted partners. The FedCIRC has stressed the importance of its trusted relationships – which cannot be recreated overnight.

The FedCIRC has established a strong partnership with organizations operating Defense and National Security systems, and has provided valuable information and advice to Federal civilian agencies regarding information security threats and vulnerabilities. The overarching purpose of FISMA is to further the development of Federal government

oversight and accountability for information security. This purpose aligns with the FedCIRC's responsibility and thus seems to be a statute that should include explicitly the FedCIRC and GSA's role. Therefore, we believe that the term "Federal information security incident center" as used in the Act should be changed to explicitly state "General Services Administration, Federal Technology Service, Federal Computer Incident Response Center".

Mr. Chairman, we appreciate your leadership, and that of the committee, for helping us achieve our goals and allowing us to share information that we feel is crucial to the protection of our nations technology resources.